TUGAS AKHIR – KS 141501

ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING

INDONESIA MALWARE ATTACK ANALYSIS IN 2013 WITH FREQUENT ITEMSET MINING METHOD

ROWI FAJAR MUHAMMAD
NRP 5212 100 080

Dosen Pembimbing I
Bekti Cahyo Hidayanto, S.Si., M.Kom.

Dosen Pembimbing II
Renny Pradina K. S.T.,M.T.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

TUGAS AKHIR – KS141501

ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING

Rowi Fajar Muhammad
5212 100 080

Dosen Pembimbing I
Bekti Cahyo Hidayanto, S.Si., M.Kom.
Dosen Pembimbing II
Renny Pradina K. S.T.,M.T.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS141501

INDONESIA MALWARE ATTACK ANALYSIS IN 2013 WITH FREQUENT ITEMSET MINING METHOD

Rowi Fajar Muhammad
5212 100 80

Supervisor I
Bekti Cahyo Hidayanto, S.Si., M.Kom.

Supervisor II
Renny P. Kusumawardani, S.T., M.T.

INFORMATION SYSTEMS DEPARTMENT
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2016

LEMBAR PENGESAHAN

ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Rowi Fajar Muhammad
5212 100 080

Surabaya, Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom.
NIP 19650310 199102 1 001

LEMBAR PERSETUJUAN

ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Rowi Fajar Muhammad
5212 100 080

Disetujui Tim Penguji: Tanggal Ujian: - 2016
Periode Wisuda: September 2016

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Pembimbing I)**

Renny P. Kusumawardani., S.T.,M.T. **(Pembimbing II)**

Dr.Eng.Febrilliyan Samopa, S.Kom., M.Kom **(Penguji I)**

Nisfu Asrul Sani, S.Kom., M.Sc. **(Penguji II)**

ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING

Nama Mahasiswa : Rowi Fajar Muhammad
NRP : 5212100080
Jurusan : Sistem Informasi FTIF-ITS
Pembimbing 1 :Bekti Cahyo Hidayanto, S.Si., M.Kom.
Pembimbing II : Renny Pradina K., S.T.,M.T.

ABSTRAK

Pertumbuhan pengguna internet di Indonesia semakin mengingkat sehingga potensi ancaman juga meningkat. Berdasarkan data-data yang dirilis oleh Sophos, Indonesia merupakan salah satu negara yang memproduksi serangan terbanyak. Untuk mendeteksi serangan pada jaringan internet, dibutuhkan Network Intrusion Detection Systems yang akan mendeteksi serangan yang datang. Serangan tersebut memiliki variasi yang cukup banyak dan menghasilkan data yang sangat besar.

Dari data serangan, maka serangan tersebut dihitung frekuensinya. Semakin tinggi maka serangan tersebut dikatakan rutin sehingga potensi ancamannya cukup besar. Pada penelitian ini, untuk mendapatkan frekuensi dari seangan tersebut dilakukan penggalian data dengan Frequent Itemset Mining. . Penelitian ini menggunakan dua algoritma, yaitu Apriori dan FP-Max. FP-Max digunakan untuk mencari kumpulan serangan apa saja yang sering tercapai sedangkan Apriori digunakan untuk menghitung frekuensinya.

Diharapkan dengan adanya penelitian ini para anlis dapatmelakukan tindaka n prevfentif terhadap jenis jenis serangan yang frekeuntif.

Itemset Mining, FP-MAX, Apriori, SNORT,Intrusion Detection Systems

INDONESIA MALWARE ATTACK ANALYSIS IN 2013 WITH FREQUENT ITEMSET MINING METHOD

Student Name : Rowi Fajar Muhammad
Student No. : 5212100080
Department : Information Systems, ITS
Supervisor 1 :Bekti Cahyo Hidayanto, S.Si., M.Kom.
Supervisor 2 : Renny Pradina K., S.T.,M.T.

ABSTRAK

Netwrok Intrusion Detection systems is a tool for detecting attack that occur in internet. Network Intrusion Detection Systems often produce a lot of data from these attack. From Network Intrusion Detection Systems, the attack may vary in attak variant.

From these attack, each attack will be computed on its frequeny. The higher frequency its attack, the higher risk will ocure. In this research, for finding its frequency we use Frequent Itemset Mining. We use two algorithm, Apriori and FP-Max. Apriori used for finding frequency for each attack and FP-Max used for finding maximal pattern that occure in every day. From this research, we found that some largest known attack is not frequent. Also, the result from Apriori and FP-Max with same minimum support remain same. Finally, we expect from this research the security analyst will take proper action for any attack that frequently occur.

Keyword : Internet Attack, Frequent Itemset Mining, FP-MAX, Apriori, SNORT,Intrusion Detection Systems

KATA PENGANTAR

Alhamdulillah, puji syukur kepada Allah SWT yang telah memberikan kekuatan, karunia-Nya dan juga masih memberikan kesempatan bagi penulis untuk menyelasaikan buku ini dengan judul " **ANALISIS MALWARE ATTACK DI INTERNET INDONESIA PADA TAHUN 2013 DENGAN METODE FREQUENT ITEMSET MINING".**

Buku ini merupakan sebuah puncak dari segala daya dan upaya penulis selama hidup dalam manisnya dunia perkuliahan. Puncak dari idealisme dan juga impian, bahwa empat tahun yang ideal haruslah bermanfaat. Ketika dulu para pejuang melakukan angkat senjata, lalu generasi selanjutnya mengangkat pena, maka generasi saya menekan tuts keyboard.

Semoga dari buku ini bermanfaat bagi Id-SIRTII/CC sebagai pemantau dunia internet di Indonesia, khususnya dalam bidang pengawasan dan penindakan kejahatan cyber. Harapannya, buku ini dapat menginspirasi kemajuan teknologi di Indonesia, khususnya dibidang keamanan teknologi informasi, komputasi terdistribusi dan penggalian data serta analisa data.

Tak lupa dalam kesempatan ini penulis mengucapkan terima kasih kepada :

- Bapak dan Ibu penulis yang memberikan dukungan penuh dan doa yang tiada henti
- Bapak Achmad Syafaat, sebagai staf Riset dan Pengembangan Id-SIRTII/CC yang selalu memberikan saran dan pertimbangan dalam penulisan buku ini
- Bapak Bekti Cahyo Hidayanto selaku dosen pembimbing I dan Ibu Renny Pradina K selaku dosen pembimbing II. Mereka telah memberikan waktu dan

juga pikiran kepada penulis untuk mengarahkan tugas akhir ini.

- Solusi247 selaku penyelenggara konferensi Id-BIG Data Indonesia yang telah menginspirasi saya dalam menggunakan Hadoop
- Bapak Faizal Johan A. selaku dosen wali saya yang selalu mengarahkan dalam hal-hal akademik saya
- Teman-teman di DPM ITS 2014/2015 yang juga saling membantu
- Teman-teman saya di SOLA12IS yang selalu saling membantu., saling memotivasi, saling memberi ilmu dan terlebih khusus saling berbagi logistik makanan dan minuman di laboratorium
- Dosen-dosen di Jurusan Sistem Informasi ITS yang telah memberikan saya pengajan ketika kuliah
- Dan tanpa mengurangi rasa hormat, saya juga berterima kasih kepada pihak-pihak yang belum saya sebutkan namanya disini

Penulis menyadari bahwa buku ini masih banyak kekurangan. Penulis memohon maaf terhadap segala kekurangan dan kekeliruan yang ada. Semoga tugas akhir ini bermanfaat bagi seluruh pembaca

Surabaya, Juni 2016

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

BAB I
PENDAHULUAN

Pada bagian pendahuluan ini, akan dijelaskan mengenai latar belakang, masalah yang akan diselesaikan, batasan masalah, tujuan serta manfaat yang dihasilkan dari Tugas Akhir ini.

1.1 Latar Belakang Masalah

Penggunaan internet tak lepas dari ancaman yang mengintai setiap saat. Dengan semakin meningkatnya pengguna internet dan juga perkembangan teknologi, maka perkembangan *malware* juga meningkat. [1]. Selain itu, ancaman lain non-*malware* juga semakin meningkat.

Ancaman dalam berinternet bukan hanya soal *malware.* Berdasarkan data yang dimiliki Symantec, pada tahun 2013 terdapat peningkatan 700% dari tahun 2012 mengenai pelanggaran privasi data pengguna. Selain itu, *website* yang memiliki *vulnerability* (kelemahan) juga mengalami peningkatan, dari 53% ditahun 2012 menjadi 77% ditahun 2013. Selain itu, jenis *vulnerability* juga bertambah, dari 5291 menjadi 6787 jenis [2].

Indonesia memiliki kondisi yang kurang baik. Indonesia masuk kedalam *Top 10 Riskiest Countries* berdasarkan laporan Sophos [3]. Indonesia memiliki *Threat Exposure Rate* (TER) sebesar 23,54%, yang berarti bahwa terdapat 23,54% dari komputer di Indonesia telah terjangkit serangan *malware.* Selain itu, Indonesia masuk kedalam 12 besar negara penyumbang *spam* terbanyak.

Is your country safe or risky?

Threat exposure rate by country

10 Safest Countries

	TER		TER
1. Norway	**1.81%**	6. U.S.	**3.82%**
2. Sweden	**2.59%**	7. Slovenia	**4.21%**
3. Japan	**2.63%**	8. Canada	**4.26%**
4. UK	**3.51%**	9. Austria	**4.27%**
5. Switzerland	**3.81%**	10. Netherlands	**4.28%**

10 Riskiest Countries

	TER		TER
1. Indonesia	**23.54%**	6. India	**15.88%**
2. China	**21.26%**	7. Mexico	**15.66%**
3. Thailand	**20.78%**	8. UAE	**13.67%**
4. Philippines	**19.81%**	9. Taiwan	**12.66%**
5. Malaysia	**17.44%**	10. Hong Kong	**11.47%**

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

Source: SophosLabs

Gambar 1.1, Top 10 Riskiest Countries

Dari laporan yang dirilis oleh Id-SIRTII/CC, pada tahun 2012 Indonesia mengalami 39 juta serangan. Serangan tersebut beragam, berupa Malware, Botnet, dan sebagainya. Rata-rata, jumlah serangan adalah 116 ribu serangan perhari. Selain itu, sebagian besar serangan didominasi oleh serangan yang sangat berbahaya. Serangan tersebut didominasi oleh serangan SQL.

Penelitian ini bertujuan untuk mengetahui bagaimana karakteristik serangan pada internet di Indonesia. Setelah mengathui karakteristik data tersebut, maka selanjutnya dipetakan hingga akhirnya dapat memberikan rekomendasi kepada pemerintah mengenai langkah-langkah antisipasi yang dapat dilakukan oleh pemerintah. Penelitian ini menggunakan data yang diambil dari data internal yang dimiliki oleh Id-SIRTII/CC. Data tersebut merupakan data dari bulan Januari hingga Oktober 2013.

Id-SIRTII/CC sebagai institusi resmi yang dibentuk oleh Kementrian Komunikasi dan Informasi yang berwenang dalam bidang ancaman gangguan kemanan internet di Indonesia telah memiliki data mengenai keamanan internet di Indonesia. Id-SIRTII/CC juga melakukan kegiatan pemantauan, sehingga ancaman-ancaman internet di Indonesa dapat diketahui, selanjutnya untuk ditindaklanjuti.

1.2 Perumusan Masalah

Rumusan masalah dalam pengerjaan Tugas Akhir ini adalah :

a. Bagaimana kondisi umum serangan internet pada trafik internet Indonesia?
b. Bagaimana distribusi persebaran serangan internet Indonesia?
c. Bagaimana karakteristik serangan internet di Indonesia?

1.3 Batasan Masalah

Batasan masalah pada tugas akhir ini adalah:

a. Data yang digunakan adalah data internal dimiliki oleh Id-SIRTII/CC pada bulan Januari-Oktober tahun 2013
b. Menggunakan sensor internal yang dimiliki Id-SIRTII/CC
c. Terbatas pada algoritma Frequent Itemset Mining, yaitu dengan algoritma Apriori dan FP-Max
d. Visualisasi data terbatas pada data serangan yang dilakukan oleh negara, bukan pada IP
e. Nilai minimum support yang digunakan untuk dikatakan *frequent* adalah minimum 95% dari jumlah hari yang ada

1.4 Tujuan Penelitian

Tujuan dari Tugas Akhir ini adalah :

a. Mengetahui kondisi umum keamanan internet di Indonesia
b. Memberikan gambaran mengenai karakteristik serangan internet di Indonesia
c. Mengetahui persebaran dari serangan internet di Indonesia
d. Memberikan rekomendasi kepada pemerintah mengenai langkah-langkah yang perlu dilakukan dalam rangka pencegahan, penanganan dan pemantauan pada internet di Indonesia

1.5 Manfaat Penelitian

Tugas akhir ini memiliki banyak manfaat, antara lain :

Untuk pemerintah :

a. Menjadi acuan bagi pemerintah, khususnya Kementran Komunikasi dan Informatika sebagai bahan dasar kajian dalam meningkatkan keamanan internet di Indonesia

b. Sebagai bahan evaluasi mengenai kondisi infrastruktur internet di Indonesia

Untuk pengguna internet :

a. Memberikan kesadaran bagi pengguna internet, khususnya di Indonesia akan bahaya tentang internet

b. Dapat menghindari akan bahaya penggunaan internet di Indonesia

1.6 Relevansi dengan Jurusan Sistem Informasi

Tugas akhir ini memiliki relevansi dengan mata kuliah Penggalian Data dan Analitika Bisnis dan Keamanan Aset Informasi. Selain itu, tugas akhiri ni juga mendukung salah satu profil lulusan JSI-ITS yaitu adalah Konsultan dan Integrator sistem. Tugas akhir ini juga memiliki relevansi dengan *roadmap* penelitian Laboratorium Infrastruktur dan Kemanan Teknologi Informasi.

"halaman ini sengaja dikosongkan"

BAB II
TINJAUAN PUSTAKA

Pada bagian tinjauan pustaka ini, akan dijelaskan mengenai referensi-referensi yang terkait dalam penyususan tugas akhir ini.

2.1 Penelitian yang Terkait

Penelitian mengenai kondisi *malware* pada negara telah rutin dilakukan oleh lembaga CERT nasional di tiap-tiap negara. Asia Pacific Computer Emergency Response Team (APCERT), sebuah lembaga yang menaungi kumpulan National CERT di negara-negara Asia Pasifik telah merilis laporan pada tahun 2013. [4] Selain itu, lembaga keamanan independen seperti Sophos, Trend Micro, dan Symantec juga telah merilis laporan tersebut rutin setiap tahunnya [3,4,6] .

Sayangnya, untuk negara Indonesia, institusi resmi yang menangani hal ini (dalam hal ini Kementrian Komunikasi dan Informatika, Direktorat Jenderal Keamanan Informasi dan Id-SIRTII/CC) belum pernah melakukan melakukan penelitian ini. Maka dari itu, penelitian ini akan membantu pihak-pihak yang terkait mengenai kondisi *malware* di Indonesia

Selain hal tersebut, terdapat beberapa penelitian ilmiah yang mengkaji mengenai *data mining* pada log SNORT. Berikut adalah tabel mengenai perbandingan penelitan yang sudah ada

Tabel 2.1 Penelitian Sebelumnya

Penulis	Judul	Metode	Hasil
Sophos [3]	Sophos Security Threat Report 2013	Dalam laporan ini, mereka tidak menyebutkan metodologi	Tren pada keamanan internet di seluruh dunia pada tahun 2013

		yang digunakan	
Trend Micro [5]	Trenlabs 3Q 2013 Security Roundup	Dalam laporan ini, mereka tidak menyebutkan metodologi yang digunakan	Tren pada keamanan internet di seluruh dunia pada tahun 2013
Symantec [2]	Internet Security Trend Report 2014	Dalam laporan ini, mereka tidak menyebutkan metodologi yang digunakan	Tren pada keamanan internet di seluruh dunia pada tahun 2013
Asia Pacific Computer Emergency Response Team [4]	APCERT Annual Report	Laporan ini merupakan gabungan laporan dari anggota APCERT sehingga tidak memberikan metodologi penelitian	Laporan masing-masing anggota APCERT di negara-negara Asia Pasifik
O.B. Remi-Omosowon [6]	Statistical Analysis for SNORT Alerts	Melakukan *Trend Analysis* untuk melihat tren yang ada pada setiap paket data yang masuk	Memberikan gambaran bagaimana *time series* bekerja pada SNORT alert. Selain itu, penelitian ini menunjukkan

			false positive yang dapat diidentifkasi dari *time series*
Risto Vaarandi and Karlis Podins [7]	Network IDS Alert Classification with Frequent Itemset Mining and Data Clustering	Melakukan *Data Clustering and Frequent Itemset Mining* pada log SNORT	Memberikan gambaran bagaimana klasifikasi dan *frequent itemset mining* mendapatkan peringatan kegiatan yang "menarik" sehingga dapat dianalisis untuk penelitian selanjutnya

2.2 Malware

Malware merupakan singkatan dari *malicious software*, sebuah tahapan-tahapan instruksi yang melakukan aktivitas mencurigakan dalam komputer. Saat ini, *Malware* merupakan ancaman yang tumbuh pesat dalam dunia computer, menghasilkan jutaan dolar dari bisnis haram ini. Pertumbuhan internet, social media dan juga pertumbuhan *botnet* yang besar telah mengakibatkan pertumbuhan *malware* secara eksponensial. [8].

Berdasarkan Ravula tahun 2011, *Malware* dapat diklasifikasikan sebagai berikut :

a. Virus

Virus merupakan program yang dapat mereplikasikan dirinya sendiri dengan cara "menempel" pada program yang berjalan. Untuk menggandakannya, dibutuhkan partisipasi pengguna komputer.

b. *Worm*

Sedikit berbeda dengan virus, *worm* merupakan program yang dapat mereplikasikan dirinya sendiri yang menyebarkan aslinannya kepada computer lain pada jaringan. Kebanyakan *worm* tidak membutuhkan partisipasi pengguna computer. Terkadang, beberapa *worm* seperti *mass-mailer* membutuhkan partisipasi pengguna

c. *Backdoor*

Backdoor merupakan program mencurigakan yang di-*install* oleh penyerang kepada target untuk mendapatkan *remote access*. Dengan kata lain, *backdoor* merupakan memungkinkan penyerang untuk melakukan *remote* kepada target. *Backdoor* dapat masuk dengan cara "menyamar" menjadi program asli.

d. *Trojan Horse* (Kuda Troya)

Trojan merupakan sebuah program yang kelihatannya baik, namun ternyata melakukan ativitas mencurigakan. Istilah ini diambil dari mitologi Yunani. Untuk menyembunyikan dari aktivitas mencurigakan, penyerang menggunakan teknik seperti mengganti dengan nama program yang biasa, memanipulasi tipe *file,* memodifikasi kode sumber program yang asli dan sebagainya. Ketuka *Trojan* ter-*install*, maka ia juga dapat melakukan instalasi *malware* lainnya.

e. *Rootkit*

Gabungan dari perilaku *Trojan* dan *backdoor* adalah *rootkit.* Selain itu, ia juga memodifikasi program lainnya pada sistem

operasi. *Rootkit* menunjukkan perilaku *Trojan* dengan menggati versi asli dari program dan juga menunjukkan prilaku yang sama dengan *backdoor* dengan membuat akses kepada penyerang untuk mengakses target secara jarak jauh

f. *Spyware*

Spyware meruapakan program yang mengumpulkan informasi rahasia dari pengguna computer, mengambil aktivitas dari *web browsing* dan mengirimkannya kepada pihak ketiga untuk keuntungan pribadi

g. *Adware*

Adware merupakan program yang menampilkan iklan yag mengganggu, seperti *pop-up, flash* dan bentuk lainnya. *Adware* terkadang juga bertindak sebagai *spyware.*

2.3 Frequent Itemset Mining

Misalnya I = {i1,i2, … , im} adalah kumpulan dari item yang ada, dan transaction database D = {T1,T2, …,Tn}, dimana Ti ($1 \leq i \leq n$) adalah transaksi yang memiliki sekumpulan I. Untuk $X \subseteq I$, transaksi T mengandung X ketika $X \subseteq T$. Set dari X merupakan itemset.

Support dari Xis adalah jumlah dari transaksi D yang memiliki X. X dikatakan frequent apabila support melebihi atau sama dengan minimum support yang diberikan [7]

Frequent Itemset Mining memiliki input yaitu *transaction database* dan juga nilai ambang batas yang dinamakan *minimum support. Transaction database* merupakan kumpulan dari ***transaksi.*** Setiap ***transaksi*** merupakan kumpulan dari ***items.*** Dalam satu ***transaksi*** tidak boleh ada ***item*** yang berulang.

2.3.1 Apriori

Apriori merupakan salah satu algoritma dalam mencari *frequent itemset* dalam *database* transaksional [9]. Algoritma ini dibuat untuk menangani *database* yang berukuran besar. [10]

Apriori akan mencari itemset yang muncul secara terus-menerus yang muncul sekurang-kurangnya nilai ***minimum support*** dari ***transaction database.*** [10]

2.3.2 FP-Max

FP-Max merupakan salah satu algoritma *Frequent Maximal Itemset.* Ia merupakan solusi dari FP-Growth yang akan mencari *pattern* yang maksimal dari tiap-tiap rule yang ada. Untuk melihat algoritmanya, lihat pada kode 2.1

```
Algorithm FPMAX (Input  T : FP-Tree; Output  M : MFI-Tree)
Variable
MFIT : MFI-Tree;
Head , Tail : Linked list of items;
Begin
if
 (T contains a single path P)
    Insert (Head U P) in MFIT
else
for (each i in header-tabel of T)
     Append i to Head;
     Construct the conditional pattern base B[i] for [i];
     Tail = {frequent items in B[i]};
if Not(Head U Tail in MFIT )
           Construct the FP-Tree T[head];
            FPMAX(T[head]);
endif;
     remove i from Head;
endfor;
endif;
End;
```

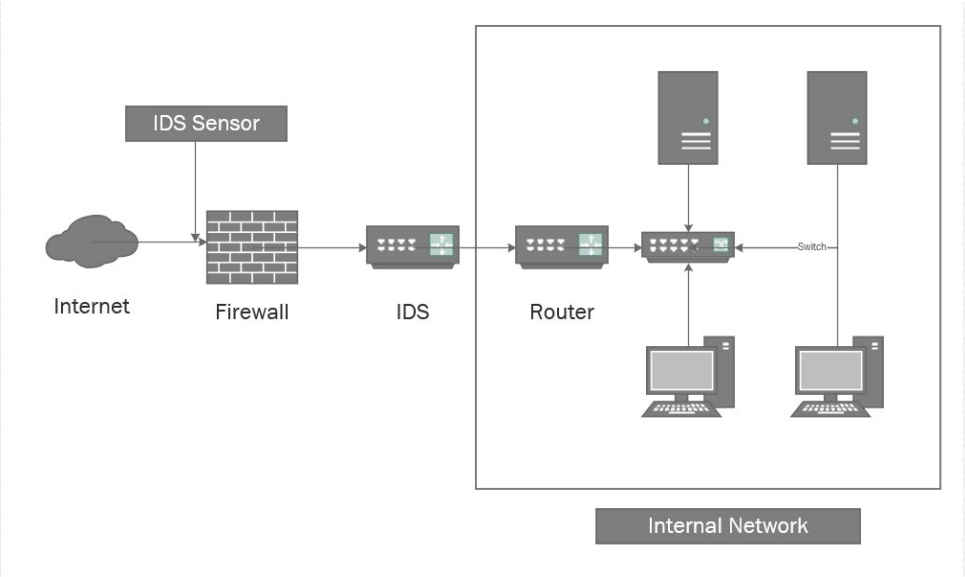
Kode 2 1. Algoritma FP-Max [11]

2.4 Intrusion Detection System (IDS)

Intrusion Detection Systems (IDS) merupakan sistem yang berfungsi untuk memonitor jaringan dengan mencari penggunaan yang tak sesuai (*unauthorized usage), denial of service (DoS)* dan anomali lainnya. Selain itu, dalam IDS memiliki tujuan utama, yaitu mengklasifikasian aktivitas sistem menjadi dua kategori, normal dan aktivitas mencurigakan (*suspicious/intrusion)*. Dalam penelitian ini, yang akan dibahas adalah kategori mencurigakan. [12]

Berbeda dengan *firewall,* ia merupakan benteng pertahanan dari jaringan komputer. *Firewall* biasanya membuat alur dari *traffic internet* dengan menginspeksi *header* dari paket data, namun tidak melihat konten, seperti adanya *mailicious software* pada paket data tersebut. Sehingga, IDS ditaruh pada luar dan dalam *firewall* dan pada akhirnya menjadi *best practice* pada implemetasi keamanan jaringan.

IDS juga dapat dikategorikan sebagai dua kategori :*host based-IDS* (HIDS) dan juga *network-based IDS* (NIDS). HIDS melakukan pemindaian *resource* dari *host machine* untuk informasi yang berkaitan dengan keamanan seperti *application logs, system activities, and file system modification logs*. NIDS memonitor *network traffic* dari serangan, biasanya IP *network packet headers.* Sehingga, NIDS melihat aktivitas dari *packet header* tersebut dan membuat keputusan mengenai apakah paket data tersebut mencurigakan atau tidak. IDS yang digunakan oleh Id-SIRTII/CC berbasis NIDS dan juga menggunakan SNORT sebagai basis IDS. Gambar dibawah merupakan contoh dari arsitektur IDS.



Gambar 2.1 Contoh ArsitekturIDS

SNORT merupakan salah satu dari aplikasi keamanan. SNORT memiliki tiga fungsi, yaitu *packet sniffer, packet logger* ataupun *Network Intrusion Detection Systems* (NIDS). SNORT bekerja pada protocol TCP/IP. SNORT [6]juga memiliki *add-ons* yang dapat ditambah sesuai kebutuhan pengguna.

SNORT memiliki tiga fitur, yaitu :

a. The Preprocessors

The preprocessors merupakan *plug-in* dari SNORT yang berfungsi untuk melakukan *parsing* dari setiap data yang datang sehingga data tersebut dapat dilihat. Bila menjalankan SNORT tanpa *snort.conf* (*preprocessor file)* maka yang dapat dilihat hanya paket data biasa tanpa mengetahui apakah paket data tersebut berbahaya ataupun tidak.

b. The Detection Engine

Detection engine merupakan fungsi utama SNORT sebagai NIDS. *Detection engine* mengambil data dari *packet decoder* dan juga *preprocessor*, lalu membandingkan hasil tersebut sehingga dapat diketahui apakah paket data tersebut berbahaya ataupun tidak.

c. The Alerting and Logging Components

Setelah mengetahui data tersebut berbahaya ataupun tidak, maka dapat selanjutnya adalah komponen untuk memperingatkan dan juga melakukan *logging.* Peringatan inilah yang dapat disimpan dalam bentuk *database.* Hal inilah yang akan dibahas dalam penelitian ini

2.5 SPMF

SPMF merupakan tool untuk melakukan data mining [13]. SPMF menggunakan Java sebagai platformnya. SPMF juga bersifat opensource sehingga dapat dimodifikasi dan didistribusikan dengan lisensi GPL v3.

2.6 Apache Hadoop

Apache Hadoop merupakan sebuah software open source framework untuk mendistribusikan penyimpanan dan juga pemrosesan kedalam sebuah cluster computer. Hadoop memiliki dua hal penting, yaitu HDFS dan MapReduce.

Hadoop File System (HDFS) merupakan sebuah filesystem yang dapat menyimpan data yang besar dengan melakukan *scaling* kedalam sebuah cluster dari beberapa hosts. HDFS menyediakan replikasi diantara tiap-tiap hostnya.

MapReduce merupakan paradigma pemrosesan data bagaimana data di input dan output dalam dua langkah, yang dikenal dengan map dan reduce. MapReduce terintegrasi dengan HDFS sehingga memastikan bahwa MapReduce akan berjalan pada node HDFS yang membutuhkan data tersebut. [14]

2.7 Apache Hive

Hive merupakan aplikasi data-warehouse yang berjalan diatas Hadoop dengan menggunakan kueri SQL. Ia juga menggunakan Mapreduce sebagai algoritma pemrosesannya. [15]

2.8 Id-SIRTII/CC

Indonesia Security Incident Response Team/Coordination Center merupakan sebuah lembaga negara yang dibentuk oleh Kementrian Komunikasi dan Informatika tahun 2007. Ia terbit melalui Peraturan Menteri Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Berdasarkan fungsinya, ia memiliki ruang lingkup sebagai berikut [16]

a. Melakukan sosialisasi kepada seluruh pihak yang terkait untuk melakukan upaya pengamanan terhadap pemanfaatan infrastruktur dan jaringan telekomunikasi berbasis protokol internet;

b. Melakukan koordinasi pencegahan, pemantauan, pendeteksian dan peringatan dini terhadap ancaman dan gangguan serta penanganan insiden pada jaringan telekomunikasi berbasis protokol internet khususnya infrastruktur strategis;

c. Melakukan pembangunan dan atau penyediaan, pengoperasian, pemeliharaan dan pengembangan sistem database, analisis, pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet yang antara lain berfungsi untuk mendukungan kegiatan pemantauan, menyimpan rekaman transaksi (log file) serta mendukung penegakan hukum;

d. Melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet dan memberikan pelayanan konsultasi dan bantuan teknis;

e. Melakukan kegiatan laboratorium pelatihan, simulasi, riset dan pengembangan di bidang pengamanan jaringan telekomunikasi berbasis protokol internet;

f. Melakukan analisa dan pengolahan data serta informasi yang dihasilkan oleh pelaksanaan pengamanan dan penanganan insiden, laboratorium, simulasi, riset dan pengembangan;

g. Melakukan kegiatan penyajian, pertukaran dan pelaporan hasil kegiatan análisis dan pengolahan data dan informasi tentang keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sesuai ketentuan peraturan perundang-undangan;

h. Menjadi pusat koordinasi nasional penanganan insiden terkait dengan ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet di Republik Indonesia.

“*halaman ini sengaja dikosongkan”*

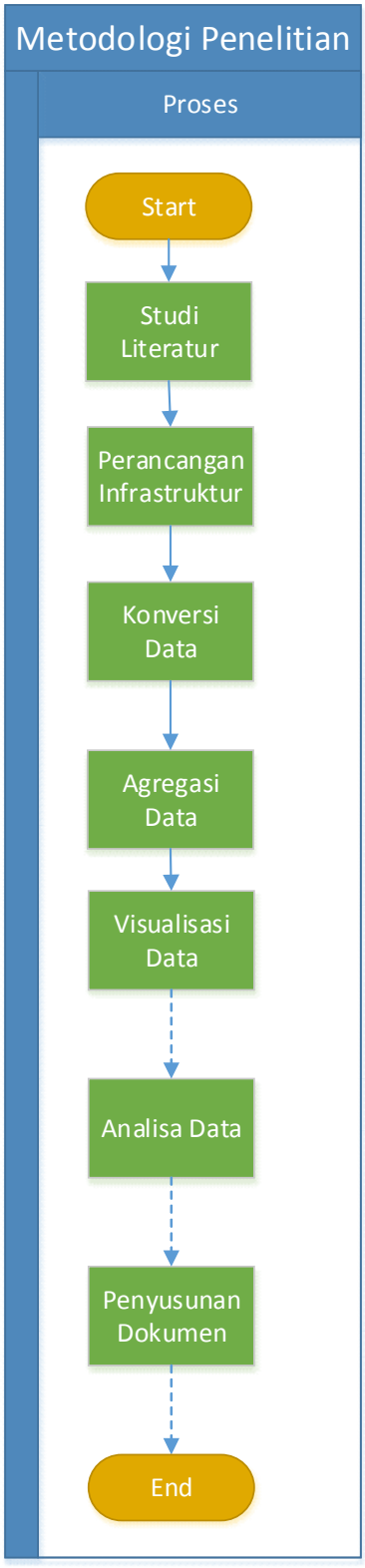
BAB III
METODOLOGI PENELITIAN

METODOLOGI PENGERJAAN TUGAS AKHIR

Pada bagian ini, akan dijelaskan mengenai metode tugas akhir yang akan digunakan dalam tugas akhir ini.

3.1 Diagram Metodologi Pengerjaan Tugas Akhir

Diagram metode pada Tugas Akhir ini ditampilkan pada gambar 3.1.



Gambar 3.1, Diagram Alur Metodologi Tugas Akhir

3.2 Penjelasan Diagram Metodologi

Berikut merupakan penjelasan dari diagram metodologi.

3.2.1. Studi Literatur

Tahap ini merupakan tahap awal dalam penelitian ini. Studi literatur dilakukan untuk membantu dalam menentukan tujuan dalam penelitian. Literatur bisa berupa buku, penelitian sebelumnya atau artikel-artikel yang mendukung. Penulis melakukan studi literatur mengenai *malware, data mining,* dan juga mengenai *SNORT beserta Intrusion Detection System*

3.2.2. Perancangan Infrastruktur

Tahap ini merupakan tahap dimana penulis melakukan proses penyiapan infrastruktur untuk mengolah data. Infrastruktur perlu disiapkan mengingat data yang besar dan mneggunakan *distributed computing*. Infrastruktur digunakan dengan batasan computer yang dimiliki oleh computer jurusan system informasi.

3.2.3. Konversi Data

Pada tahap ini data yang sudah diperoleh dari Id-SIRTII/CC dilakukan konversi kedalam bentuk geolocation dari IP yang ada dan juga dikonversi menjadi bentuk *transactional database* agar bisa dilakukan *data mining.*

3.2.4. Agregasi Data

Pada tahap ini data yang sudah diperoleh dari Id-SIRTII/CC dilakukan agregasi data. Agregasi data diperlukan untuk

3.2.5 Data Mining

Pada tahap ini, data yang telah ada ditransformasikan kedalam bentuk yang sesuai untuk diproses melalui *data mining. Data* mining bertujuan untuk mencari karakteristik data yang ada. Data yang telah sesuai dengan bentuk yang diinginkan akan dilakukan proses klasterisasi terlebih dahulu. Selain itu, juga

dilakukan *frequent itemset mining* untuk mencari serangan apa yang "menarik" untuk ditelusuri lebih lanjut dan juga keterkaitan antara satu data dengan data yang lain.

Frequent Itemset Mining dilakukan dengan dua algoritma, yaitu Apriori dan FP-Max.

3.2.6 Visualisasi Data

Data yang ada, baik yang bersifat data agregasi maupun data hasil data mining divisualisasikan. Data tersebut divisualisasikan untuk mempermudah pembacaan data dari hasil data mining dan juga data yang ada, sehingga mempermudah analisis dari data yang ada.

3.2.7 Analisa Data

Setelah itu, data yang telah divisualisasikan beserta hasil dari klasterisasi data dianalisa. Analisa ini bertujuan untuk memberikan hasil dari penelitian ini.

3.2.8 Pembuatan Buku Tugas Akhir

Tahapan ini adalah tahap paling akhir, setelah serangkaian tahapa pengerjaan tugas akhir dilakukan. Pada tahapan ini, seluruh dokumentasi hasil pengerjaan pada tahap sebelumnya dikumpulkan dan dijadikan buku tugas akhir.

BAB IV
PERANCANGAN

Pada bab ini, akan dijelaskan mengenai data yang akan diolah beserta rancangan proses pengolahannya, serta mempersiapkan sistem yang akan digunakan untuk mengolah data.

4.1. Deskripsi Data

Data yang didapatkan dari IdSIRTII/CC merupakan kumpulan dari log Intrusion Detection System yang dimiliki oleh mereka, yaitu SNORT. Jumlah data yang ada adalah sebanyak 41.888.232 data. Secara umum, data ini memiliki header sebagai berikut:

1. Message

Deskripsi: Merupakan nama jenis serangan yang terdaftar pada SNORT rule.

Keterangan: Nomor yang terdapat didalam tanda dalam kurung

’ () ’ merupakan ID dari SNORT Rule. Selain itu, huruf kapital didepan Message mengindikasikan nama jenis serangan.

2. Time

Deskripsi: Waktu terjadinya serangan

Keterangan: Waktu merupakan format timestamp yang berisi waktu serangan dan tanggal serangan

3.Destination IP

Deskripsi: Asal dari IP penyerang.

Keterangan: Dalam tuags akhir ini, IP tidak boleh dipublikasikan karena bersifat rahasia.

4. Source IP

Deskripsi: Tujuan IP dari serangan

Keterangan: Dalam tugas akhir ini, IP tidak boleh dipublikasikan

karena bersifat rahasia

5. Classification

Deskripsi: Merupakan klasifikasi dari tiap tiap jenis serangan

yang telah didefinisikan dari SNORT Rule. Klasifikasi ini sudah terdefinisikan dari SNORT Rule

Keterangan: Data ini bergantung pada SNORT Rule ID dimana otomatis ditentukan oleh mesin.

6. Priority

Deskripsi: Merupakan tingkat bahaya dari jenis serangan. Telah terdefinisi dari mesin.

Keterangan: Data ini memiliki tiga variabel, yaitu high, medium dan low

7.Destination Port/ICMP Code

Deskripsi: Merupakan port tujuan serangan

Keterangan: -

8. Source Port/ICMP Code

Deskripsi: Merupakan port dari IP asal terjadinya serangan

Keterangan: -

9. Detection Engine

Deskripsi: Merupakan lokasi atau tempat dimana lokasi dari IDS

dipasang.

Keterangan: Dalam tugas akhir ini, nama detection engine disamarkan. Terdapat delapan lokasi detection engine

10. IP Address
Deskripsi: Data kosong.
Keterangan: Data kosong.
3

11. IPv6 Source
Deskripsi: Data kosong.
Keterangan: Data kosong.

12. IPv6 Destination
Deskripsi: Data kosong.
Keterangan: Data kosong.

13. Email Sender
Deskripsi: Data kosong.
Keterangan: Data kosong.

14. Email Recipent
Deskripsi: Data kosong.
Keterangan: Data kosong.

15. Email Attachments
Deskripsi: Data kosong.
Keterangan: Data kosong.

16. HTTP Hostname

Deskripsi: Data kosong.

Keterangan: Data kosong.

17. HTTP URI

Deskripsi : Data kosong.

Keterangan: Data kosong

Dibawah merupakan contoh potongan data dari data yang ada

Message	Time	Destination IP	Source IP	Classification	Priority	Protocol	Destination P	Source Port/I	Detection
SQL probe response overflow attempt (1:2329)	1/1/2013 7:22	SENSOR	SENSOR	Attempted User Privilege Gain	high	udp	4830/udp	14141/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:22	SENSOR	SENSOR	Attempted User Privilege Gain	high	udp	14412/udp	14141/udp	A
BOTNET-CNC Trojan.Spyeye-206 outbound connection (1:20763)	1/1/2013 7:21	SENSOR	SENSOR	A Network Trojan was Detected	high	tcp	80 (http)/tcp	26902/tcp	A
BOTNET-CNC Palevo bot DNS request attempt (1:16298)	1/1/2013 7:21	SENSOR	SENSOR	Misc Activity	low	udp	53 (domain)/u	21436/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:21	SENSOR	SENSOR	Attempted User Privilege Gain	high	udp	61995/udp	34831/udp	A
BOTNET-CNC Palevo bot DNS request for C&C attempt (1:16297)	1/1/2013 7:21			A Network Trojan was Detected	high	udp	53 (domain)/u	17027/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:20			Attempted User Privilege Gain	high	udp	4830/udp	14141/udp	A
SQL Worm propagation attempt (1:2003)	1/1/2013 7:20			Misc Attack	medium	udp	1434 (ms-sql-i	1236/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:20			Attempted User Privilege Gain	high	udp	61995/udp	34831/udp	A
BOTNET-CNC Trojan.Spyeye-206 outbound connection (1:20763)	1/1/2013 7:20			A Network Trojan was Detected	high	tcp	80 (http)/tcp	26901/tcp	A
BOTNET-CNC Palevo bot DNS request attempt (1:16298)	1/1/2013 7:20			Misc Activity	low	udp	53 (domain)/u	25436/udp	A
BOTNET-CNC Palevo bot DNS request for C&C attempt (1:16297)	1/1/2013 7:19			A Network Trojan was Detected	high	udp	53 (domain)/u	12609/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:19			Attempted User Privilege Gain	high	udp	4830/udp	14141/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:19			Attempted User Privilege Gain	high	udp	62480/udp	2267/udp	B
SQL Worm propagation attempt (1:2003)	1/1/2013 7:19			Misc Attack	medium	udp	1434 (ms-sql-i	3093/udp	A
SQL probe response overflow attempt (1:2329)	1/1/2013 7:19			Attempted User Privilege Gain	high	udp	61995/udp	34831/udp	A
BOTNET-CNC Virut DNS request for C&C attempt (1:16302)	1/1/2013 7:19			A Network Trojan was Detected	high	udp	53 (domain)/u	39599/udp	B
BOTNET-CNC Trojan.Spyeye-206 outbound connection (1:20763)	1/1/2013 7:18			A Network Trojan was Detected	high	tcp	80 (http)/tcp	26899/tcp	A
SQL Worm propagation attempt (1:2003)	1/1/2013 7:18			Misc Attack	medium	udp	1434 (ms-sql-i	3093/udp	C
SQL probe response overflow attempt (1:2329)	1/1/2013 7:18			Attempted User Privilege Gain	high	udp	50170/udp	7454/udp	C
SQL Worm propagation attempt (1:2003)	1/1/2013 7:18			Misc Attack	high	udp	1434 (ms-sql-i	3093/udp	A

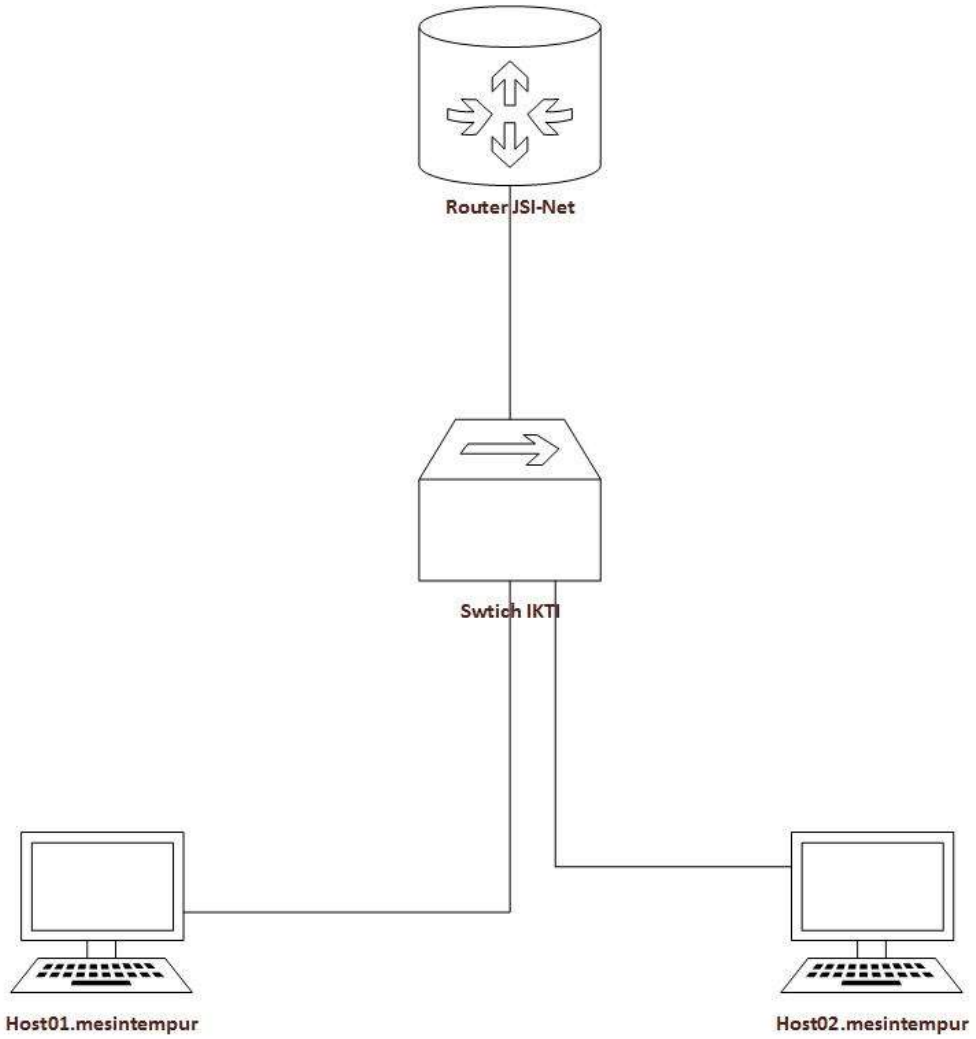
Gambar 4.1 Contoh Tampilan Data Mentah

4.2 Perancangan Infrastruktur

Untuk mengolah data dalam jumlah yang besar, maka diperlukan infrastruktur yang baik. Selain itu, dalam tugas akhir ini akan digunakan Apache Hadoop dan Apache Hive dalam mode terdistribusi untuk mendistribusikan pekerjaan.

4.2.1 Topologi Jaringan

Gambar 4.2 menjelaskan mengenai topoligi jaringan yang digunakan untuk Hadoop Distributed File System.



Gambar 4..1. Topologi Jaringan Infrastruktur Untuk Pengerjaan Tugas Akhir

4.2.2 Spesifikasi Hardware

host01.mesintempur

Processor : Core i7 4702MQ RAM : 16 GB HDD : 1 TB OS : CentOS 6.7

host02.mesintempur

Processor : Core i5 RAM : 8 GB HDD 300 GB OS : CentOS 6.7

4.2.3 Spesifikasi Software

a. Apache Hadoop 2.3.0

b. Apache Ambari

c. Apache Hive2

d. Apache Sqoop

4.3 Instalasi Software

Pada tahap ini menjelaskan instalasi dilakukan pada infrastruktur yang telah dirancang. Instalasi dilakukan dengan menggunakan *software* Apache Ambari. Apache Ambari berguna untuk memudahkan manajemen aplikasi Hadoop, termasuk pada instalasi, monitoring dan manajemen cluster. Pada Apache Ambari, yang penting untuk diinstall adalah Apache Hadoop sebagai basis penyimpanan dan juga pemrosesan data dan juga Apache Hive sebagai tool untuk menyimpan serta sebagai *interface* antara data yang ada dengan kueri SQL-Like.

Berikut adalah software-software yang perlu diinstall untuk Tugas Akhir ini

1. Apache Ambari
2. Apache Hadoop
3. Apache Hive
4. Apache Sqoop
5. YARN
6. MapReduce

4.4 Migrasi Data

Data yang diperoleh dari Id-SIRTII/CC merupakan file MDF yang mana merupakan *database* dari Microsoft SQL Server 2012. Agar data tersebut dapat diolah dengan menggunakan

Apache Hadoop dan Apache Hive, maka data tersebut perlu dimigrasi ke Apache Hive.

Untuk melakukan migrasi, maka jalankan Apche Sqoop dengan user HDFS sebagaimana pada Kode 4.1 Untuk mengimpor, diperlukan Microsoft SQL JDBC Driver versi 4.

```
sqoop import --connect
"jdbc:sqlserver://10.126.xx.xx;
database=malware-fire" -username "sa" -P --
driver "com.
microsoft.sqlserver.jdbc.SQLServerDriver" --
target-dir /
user/forTA/ALL_ROW_REPORT_2013 --query
"SELECT * FROM
dbo.ALL_ROW_REPORT_2013 WHERE \$CONDITIONS"
-m 2
```

Kode 4.1 Skrip Mengimpor dari SQL Server ke Apache Hive

4.5 Konversi Data

Pada sub-bagian ini akan dijelaskan mengenai konversi data, yaitu data IP menjadi geolocation dan mengubah bentuk *log database* menjadi data transaksional yang dapat diolah menjadi Frequent Itemset Mining

4.5.1 Konversi IP Menjadi Geolocation

Untuk mengetahui lokasi penyerang dan tujuan penyerang beserta jumlah serangan dari masing-masing tiap negara, maka perlu untuk melakukan konversi dari IP menjadi geolocation. Untuk melakukan konversi IP menjadi IP Geolocation, maka perlu API dan database geolocation tersebut. Pada tugas akhir ini menggunakan *database* versi gratis dari Maxmind dan juga menggunakan API dari Maxmind [17]

Proses konversi diawali dengan melakukan agregasi data IP penyerang dan IP tujuan. Setelah IP penyerang dan IP tujuan diagregasi, maka selanjutnya dikonversi menjadi data Geolocation berupa nama negara, nama kota dan juga koordinat. Pada kode 4.2 dijelaskan mengenai proses konversi dengan menggunakan Java.

```
/*
This function generate an IP Address into
geolocation
data, such as country name, city name,
latitude
, longitude and ISO Code for country. It
depends
on IP Geolocation databse, provided by
Maxmind.
*/

public void getLocation(String ipAdd) throws
IOException, GeoIp2Exception{
try{
/*Checking the database file*/
File file = new File("GeoLite2-City.mmdb");
DatabaseReader reader = new
DatabaseReader.Builder(file).build();
InetAddress ipAddress =
InetAddress.getByName(ipAdd);

/* The conversion proces s*/

CityResponse responsea =
reader.city(ipAddress);
Country country = responsea.getCountry();
City city = responsea.getCity();
Location location = responsea.getLocation();
10
IsoCode = (country.getIsoCode());
CountryName =(country.getName());
GeoNameId = (country.getGeoNameId());
CityName =(city.getName());
Latitude = (location.getLatitude());
```

```
Longitude = (location.getLongitude());
}



catch(IOException e){
System.out.println("File Not FOund");
}
 /*A Java Program exception if the IP
Address is not
exists*/
```

Kode 4.2. Potongan Kode Konversi IP Menjadi GeoLocation

4.5.2 Konversi Menjadi Transactional Database

Data yang ada memiliki bentuk seperti pada gambar 4.3 sehingga perlu diubah menjadi sebuah dataset transaksi. Dataset tersebut merupakan jenis-jenis serangan yang ada pada satu hari. Setiap baris pada dataset tersebut merupakan satu transaksi, yaitu adalah satu hari. Sedangkan isi dari baris tersebut merupakan SNORT Rule ID yang mewakili jenis serangan yang akan digalu keterkaitannya.

Untuk melakukan hal tersebut, maka kode 4.3 melakukan proses konversi data tersebut menjadi bentuk database transaksional.

```
public static void generator(String path){
File file = new File(path);
List<String> lines =
Files.readAllLines(file.toPath(),
StandardCharsets.UTF_8);
List<String> msg = new ArrayList();
for(int i=1;i<lines.size();i++){
String line = lines.get(i);
String [] readline = line.split(",");
String message = readline[0];
String pattern="";
if(message.contains("(")){
pattern =
message.substring(message.indexOf("
(")+1,message.indexOf(")"));
pattern = pattern.replace(":", "");
msg.add(pattern);
}
else{}
}

count(msg);
catch(Exception e){
System.out.println(e.getMessage());
em.out.println(e.getMessage());
```

Kode 4.3 Potongan Kode Ekstraksi Rule Number dari Tiap Message di ALL_ROW_REPORT

4.6 Agregasi Data

Sebelum melakukan pre-processing untuk penggalian data, maka
agregasi data diperlukan untuk mengetahui hal-hal yang bersifat umum dari data yang ada. Agregasi data dilakukan dengan menggunakan SQL Query. Hasil agregasi juga dapat dijadikan acuan dalam melakukan pembuatan visualisasi

4.7 Visualisasi

Untuk mengetahui kondisi gambaran umum internet di Indonesia, maka diperlukan visualisasi untuk mempermudah analisis. Visualisasi yang diharapkan adalah visualisasi berupa penggambaran peta serangan, negara mana saja yang menyerang dan juga negara mana saja yang menjadi tujuan serangan.

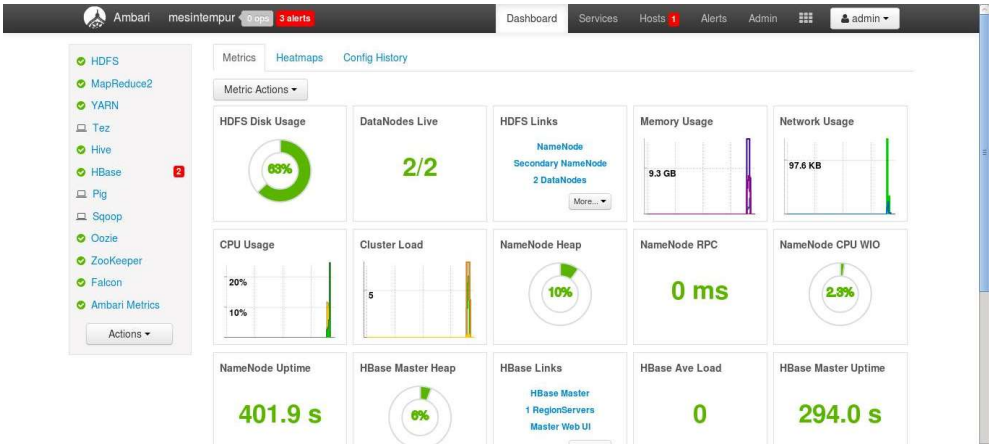
Selain itu, perlu digambarkan mengenai jenis serangan yang ada dan juga data periodic jumlah serangan tiap hari dan tiap bulannya.

BAB V
IMPLEMENTASI

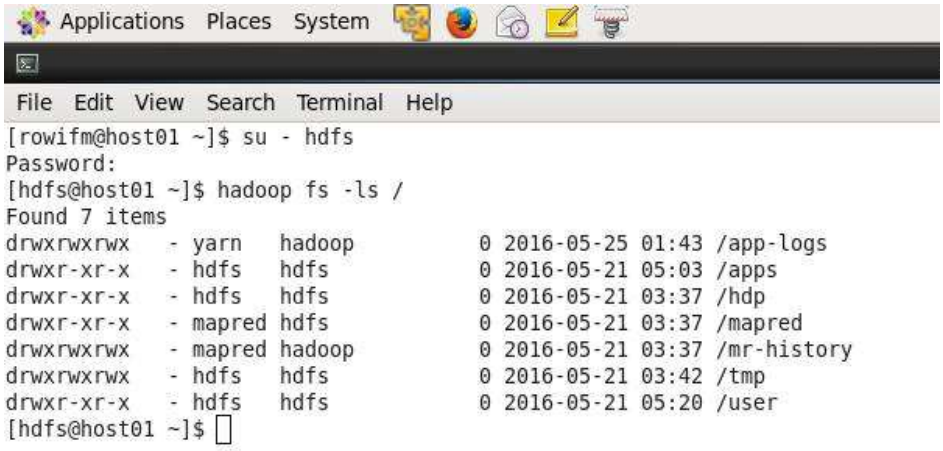
Pada bab ini akan dijelaskan proses pengolahan data yang didapatkan dari tahap rancangan sebelumnya dan juga proses implementasi dari instalasi Apache Hadoop dan Hive, migrasi data, agregasi visuliasi dan *frequent itemset mining*.

5.1 Hasil Instalasi Apache Ambari

Gambar 5.1 merupakan screenshot pada Apache Ambari. Pada dashboard tersebut terlihat berbagai aplikasi yang ada diatas Hadoop. Sedangkan untuk melakukan pengecekan apakah Hadoop berjalan, maka dapat dilakukan perintah untuk melihat seluruh direktori seperti pada gambar 5.2



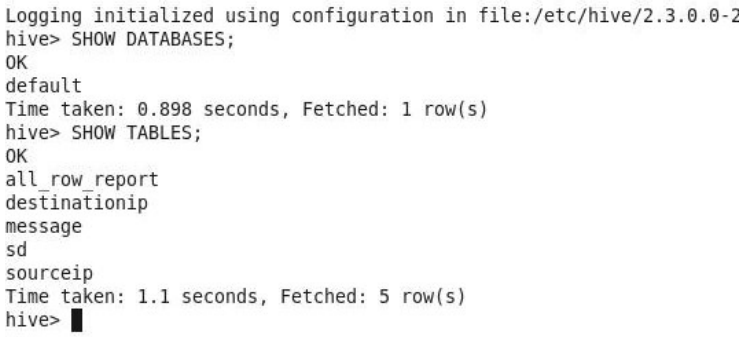
Gambar 5.1 Dashboard Apache Ambari



Gambar 5.2 Perintah Hadoop List Direktori

5.2 Migrasi Data

Untuk melakukan pengecekan data, maka perlu untuk melihat pada database Hive. Data yang dipindah merupakan data dari Microsoft SQL ke Apache Hive dengan nama tabel ALL_ROW_REPORT. Untuk melakukan pengecekan apakah data tersebut berhasil dimasukkan atau tidak, dapat dilakukan perintah pada Hive dengan "SHOW TABLES" seperti pada gambar 5.3



Gambar 5.3 Show Tables Apache Hive

5.3 Konversi Data

Konversi data dilakukan untuk mengubah suatu bentuk data menjadi bentuk data lain agar data tersebut dapat diolah. Pada tugas akhir ini, proses konversi dibagi menjadi dua, yaitu mengonversi IP menjadi data *geolocation* dan mengubah data mentah menjadi *transational database* yang bisa dilakukan penggalian.

5.3.1 Konversi IP Menjadi Geolocation

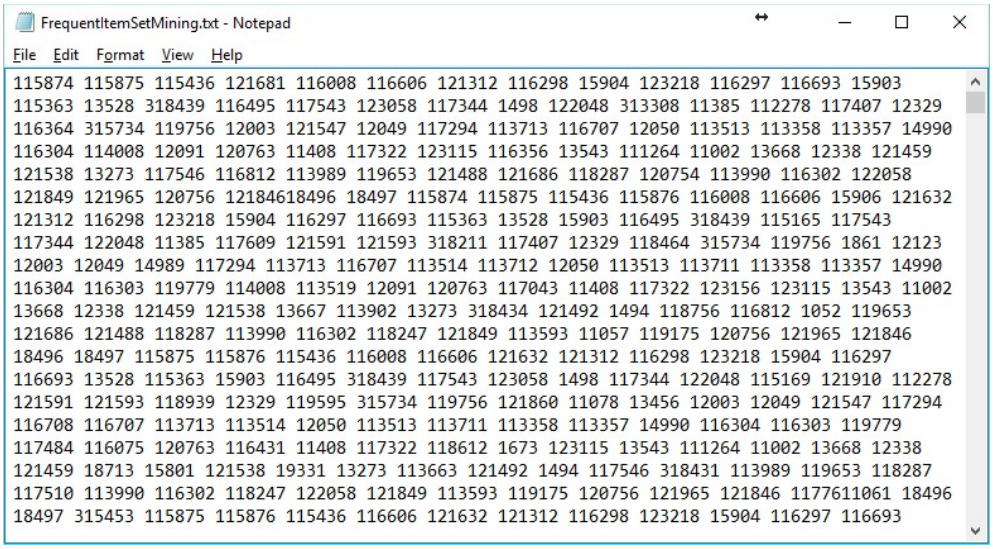
Proses konversi IP menjadi Geolocation dilakukan dengan menggunakan API dari Maxmind [17]. API tersebut berjalan dengan program Java dan membutuhkan database dari Maxmind. Maxmind menawarkan opsi gratis dan berbayar. Untuk tugas akhir ini, database yang digunakan adalah versi gratis sehingga akurasinya berkurang.

Hasil IP beserta jumlah kejadian dan geolocation dimasukkan dalam database lain. Database tersebut bernama "Source IP" dan "Destination IP". Hal ini dimaksudkan agar data mentah tidak termodifikasi. Hasil dari konversi tersebut dapat dilihat pada sub-bab 5.6

5.3.2 Konversi Menjadi Transaction Database

Proses pengubahan dari database menjadi ***transactional database*** dilakukan dengan program Java. Adapun untuk melihat kode sumber dapat melihat lampiran D. ***Transactional database harus memiliki nilai integer*** sehingga SNORT Rule yang ada dimodifikasi sedikit hingga dapat diolah. SNORT Rule tersebut dipisahkan oleh spasi dan dipisahkan oleh baris baru pada hari yang berbeda

Gambar 5.4 merupakan tampilan ***transaction database*** yang dihasilkan



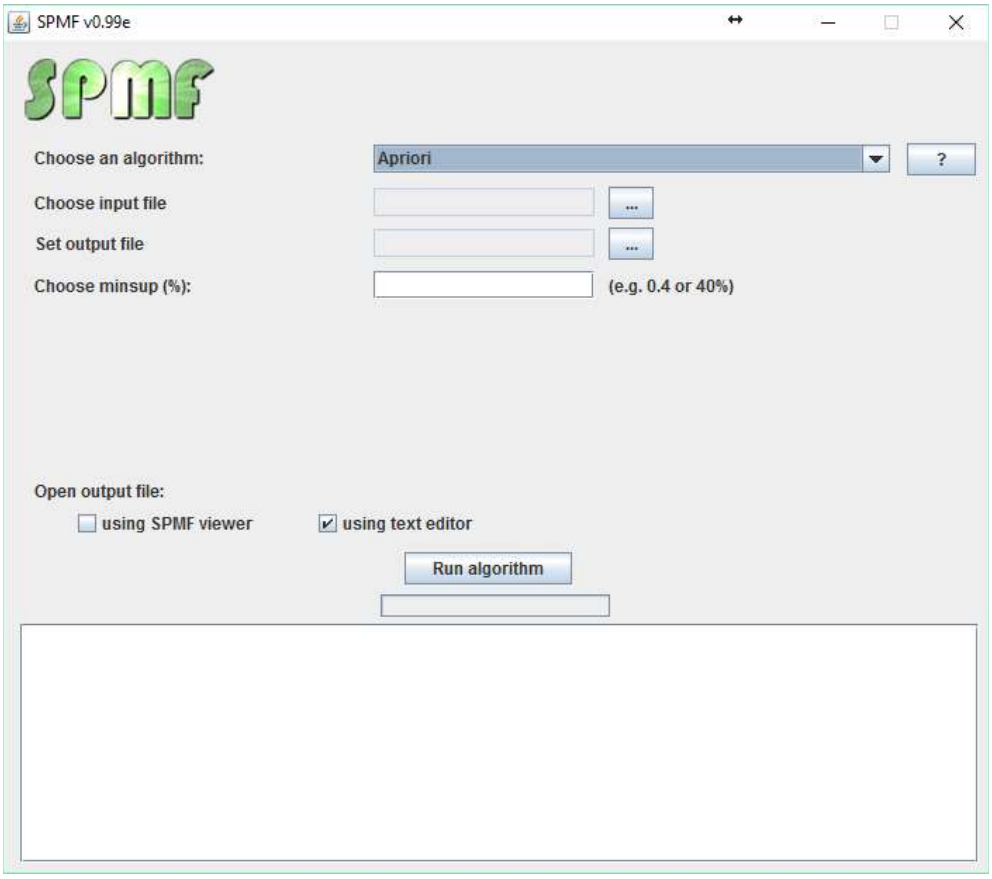
Gambar 5.4 Contoh Transaction Databse

5.4 Frequent Itemset Mining Dengan SPMF

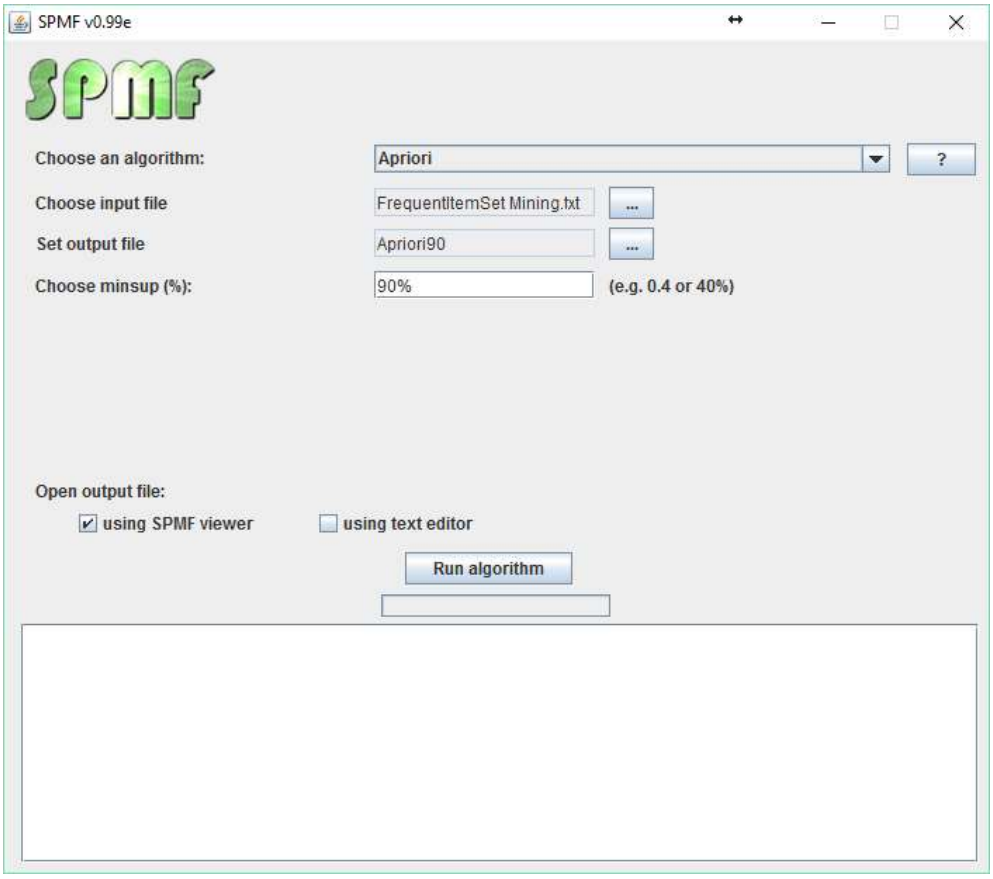
SPMF merupakan tool data mining yang dibuat oleh Philippe Fournier-Viger yang mengimplementasikan berbagai algoritma data mining kedalam bentuk program Java [9]. Ia memiliki 119 algoritma untuk :

- **association rule mining,**
- **itemset mining,**
- **sequential pattern mining,**
- **sequential rule mining,**
- **sequence prediction**,
- **high-utility pattern mining,**
- **clustering** and **classification**

Gambar 5.5 dan 5.6 merupakan contoh tampilan SPMF.



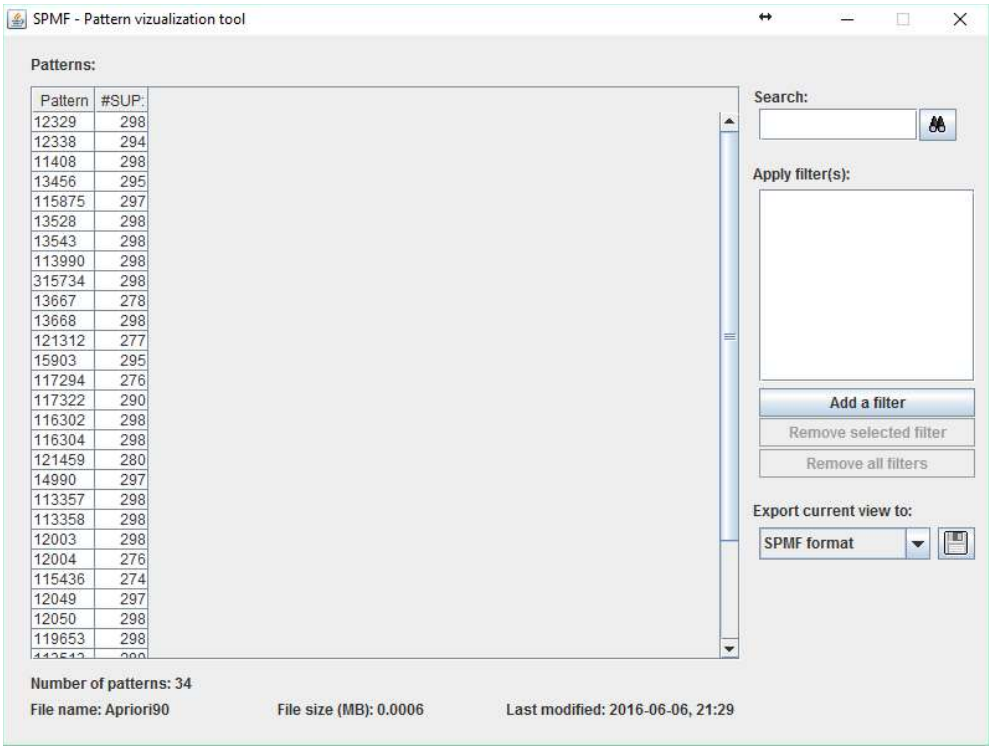
Gambar 5.5 Tampilan Awal SPMF



Gambar 5.6 Tampilan SPMF

5.4.1 Hasil Algoritma Apriori

Berikut adalah hasil algoritma Apriori dengan minimum support 70%. Gambar 5.7 merupakan output dari program SPMF



Gambar 5.7 Tampilan SPMF

Pada tabel 5.1 merupakan hasil dari Algoritma Apriori dengan minimum support 70%. Sedangkan pada tabel 5.2 merupakan hasil algoritma apriori dengan minimum support sebesar 70%

Minimum Support	Jumlah Pattern
70%	50
75%	43
80%	37
85%	35
90%	34
95%	26
99%	20
100%	17

Tabel 5.1 Hasil Algoritma Apriori Dengan Minimum Support 70%

Pattern	Persentase
12329	100
11408	100
13528	100
13543	100
113990	100
315734	100
13668	100
116302	100
116304	100
113357	100
113358	100
12003	100
12050	100
119653	100
116693	100
13273	100
121849	100
115875	99.66443
14990	99.66443
12049	99.66443
13456	98.99329
15903	98.99329
12338	98.65772
121846	97.98658

117322	97.31544
113513	96.97987
121459	93.95973
116707	93.95973
13667	93.28859
121312	92.95302
117294	92.61745
12004	92.61745
115436	91.94631
116606	91.94631
122048	87.91946
11057	82.55034
11002	80.53691
124255	79.19463
123493	79.19463
124908	79.19463
125476	78.85906
114008	77.85235
121593	75.50336
113514	74.49664
116297	73.15436
116298	72.81879
122063	72.14765
11776	71.81208
14989	70.4698
125471	70.13423

5.4.2 Hasil Algoritma FPMax

Tabel 5.2 merupakan perbandingan jumlah pattern dengan minimum support.

Tabel 5.2 Perbandingan Nilai Minimum Support Dengan Jumlah Pattern

Minimum Support	Jumlah Pattern
70%	665
75%	423
80%	237
85%	120
90%	48
95%	10
99%	1
100%	0

Dapat terlihat bahwa semakin tinggi nilai support, maka semakin sedikit pula pattern yang muncul. Sebuah pattern dapat dikatakan adalah sebuah pattern apabila ia merupakan subset dari sebuah pattern. Namun, FP-Max mencari jumlah pattern yang maksimal sehinga pattern tersebut tidak dapat dicari subset-nya lagi. Untuk mendapatkan jenis serangan yang *frequent* dan juga mengurangi *redudansi*, maka nilai support perlu ditingkatkan. Nilai support yang digunakan dalam algoritma ini adalah 95% dan 99%.

Berikut pada tabel 5.3 merupakan hasil pada minimum support 95%

Tabel 5.3 Hasil Algoritma FP-Max dengan Minimum Support 95%

Pattern	Support
	%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 12338 113513	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 15903 113513	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 13456 113513	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 115875 12338 121846 117322	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 115875 15903 12338 117322	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 12338 117322	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 115875 13456 15903 117322	95.30%

11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 15903 117322	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 13456 117322	95.30%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875 13456 15903 12338 121846	95.30%

Tabel 5.4 merupakan hasil dengan minimum support sebanyak 99%

Tabel 5.0.4 Hasil Algoritma FP-Max Dengan Minimum Support 99%

Pattern	Support
	%
11408 12003 12050 12329 13273 13528 13543 13668 113357 113358 113990 116302 116304 116693 119653 121849 315734 12049 14990 115875	99%

5.6 Hasil Agregasi

Bagian ini menjelaskan hasil agregasi data berdasarkan data mentah yang ada. Selain itu data hasil konversi geolocation juga digunakan dalam proses ini. Agregasi dimaksudkan untuk mencari informasi dari data log Id-SIRTII/CC tahun 2013.

5.6.1 Agregasi Berdasarkan Message yang Diterima

Berdasarkan hasil agregasi, diketahui bahwa terdapat 621 jenis serangan dengan jumlah yang sangat bervariasi, yaitu dari minumum 1 hingga 15.776.139 dengan rataan sebanyak 67.346. Tabel ?? menampilkan 100 jenis serangan terbanyak dan juga jumlahnya. Untuk melihat hasil lengkap dapat melihat Lampiran A

Tabel 5.5 100 Jenis Serangan Terbanyak

No	Message	Jumlah
1	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication (1:23493)	15,776,139
2	SERVER-MSSQL probe response overflow attempt (1:2329)	8,416,882
3	SQL Worm propagation attempt (1:2003)	2,695,211
4	SERVER-MSSQL version overflow attempt (1:2050)	2,662,901
5	SERVER-MSSQL heap-based overflow attempt (1:4990)	2,275,018
6	SQL Worm propagation attempt OUTBOUND (1:2004)	2,250,726
7	SQL SA brute force login attempt TDS v7/8 (1:3543)	2,249,253
8	MALWARE-CNC ZeroAccess Spiral Traffic (1:25471)	1,003,710
9	MALWARE-CNC Virut DNS request for C&C (1:16302)	536,264
10	MALWARE-CNC Virut DNS request (1:16304)	535,521

No	Message	Jumlah
11	MALWARE-CNC Possible host infection - excessive DNS queries for .ru (1:21545)	453,291
12	MALWARE-CNC Sality logo.gif URLs (1:24255)	258,430
13	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693)	220,347
14	MALWARE-CNC Trojan-Downloader.Win32.Bulknet.A outbound connection (1:21227)	212,544
15	MALWARE-CNC Trojan.Zeus P2P outbound communication (1:22048)	210,158
16	SQL sa brute force failed login unicode attempt (1:3273)	193,250
17	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)	166,003
18	OS-WINDOWS Microsoft Windows NAT Helper DNS query denial of service attempt (1:17294)	121,177
19	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt (1:19653)	115,072
20	BLACKLIST USER-AGENT known malicious user-agent string Opera/8.89 - P2P-Worm.Win32.Palevo.ddm (1:19756)	97,684
21	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)	94,932
22	SQL probe response overflow attempt (1:2329)	84,223

No	Message	Jumlah
23	MALWARE-CNC Possible host infection - excessive DNS queries for .cn (1:21546)	70,953
24	SQL generic sql insert injection atttempt - GET parameter (1:13513)	65,755
25	MALWARE-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)	61,904
26	BLACKLIST User-Agent known malicious user agent - User-Agent User-Agent (1:25476)	60,439
27	SERVER-MYSQL mysql_log COM_CREATE_DB format string vulnerability exploit attempt (1:16707)	57,332
28	MALWARE-CNC Palevo bot DNS request for C&C (1:16297)	56,083
29	MALWARE-CNC Palevo bot DNS request (1:16298)	56,058
30	MALWARE-CNC Trojan.Spyeye-206 outbound connection (1:20763)	55,789
31	BAD-TRAFFIC BIND named 9 dynamic update message remote dos attempt (3:15734)	53,883
32	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)	48,706
33	DOS MSDTC attempt (1:1408)	38,689
34	MALWARE-OTHER generic IRC botnet connection (1:19362)	31,141

No	Message	Jumlah
35	SERVER-MYSQL client authentication bypass attempt (1:3668)	28,637
36	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)	28,292
37	SERVER-MYSQL protocol 41 client authentication bypass attempt (1:3667)	28,057
38	MALWARE-CNC W32.Dofoil variant outbound connectivity check (1:21312)	26,264
39	MALWARE-CNC Win.Trojan.Agent.alqt variant outbound connection (1:19484)	25,726
40	MALWARE-CNC Sality logos.gif URLs (1:25809)	23,605
41	SQL ping attempt (1:2049)	20,965
42	MALWARE-CNC Win.Trojan.Hioles.C outbound connection (1:23391)	20,524
43	MALWARE-CNC TDSS outbound connection (1:21444)	20,365
44	SERVER-OTHER IBM Tivoli Storage Manager Express Backup counter heap corruption attempt (1:15436)	17,148
45	MALWARE-CNC URI request for known malicious URI - ZBot (1:18938)	14,485
46	SQL union select - possible sql injection attempt - GET parameter (1:13990)	13,431
47	BLACKLIST Connection to malware sinkhole (1:25018)	12,973

No	Message	Jumlah
48	INDICATOR-COMPROMISE c99shell.php command request - ls (1:16627)	11,671
49	SERVER-WEBAPP PHP-CGI remote file include attempt (1:22063)	9,978
50	SERVER-MYSQL MySQL/MariaDB client authentication bypass attempt (1:23115)	9,424
51	INDICATOR-SHELLCODE x86 OS agnostic xor dword decoder (1:17344)	9,042
52	MALWARE-CNC TDS Sutra - request in.cgi (1:21846)	8,741
53	BOTNET-CNC Virut DNS request for C&C attempt (1:16302)	8,369
54	MALWARE-CNC RAT update protocol connection (1:24211)	8,249
55	MALWARE-CNC Trojan.Zbot variant outbound connection (1:23972)	8,212
56	SERVER-MYSQL create function access attempt (1:3528)	8,050
57	SQL sa login failed (1:688)	8,017
58	MALWARE-CNC Win.Trojan.DarkComet outbound connection - post infection (1:21461)	7,444
59	MALWARE-CNC Trojan.Ransom variant outbound connection (1:21632)	7,407
60	DELETED MYSQL yaSSL SSLv2 Client Hello Message Challenge Buffer Overflow attempt (1:13713)	7,338

No	Message	Jumlah
61	SERVER-MYSQL 4.0 root login attempt (1:3456)	6,812
62	BLACKLIST User-Agent known malicious user agent - Go http package (1:24439)	6,649
63	SQL generic sql with comments injection attempt - GET parameter (1:16431)	5,704
64	MALWARE-CNC Win.Trojan.Winnti.A contact to cnc server (1:20630)	5,596
65	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)	5,590
66	BOTNET-CNC Virut DNS request attempt (1:16304)	5,383
67	WEB-MISC Microsoft ASP.NET information disclosure attempt (3:17429)	5,371
68	MALWARE-CNC Trojan.Dropper-23836 outbound connection (1:21593)	5,221
69	MALWARE-TOOLS Havij advanced SQL injection tool user-agent string (1:21459)	4,855
70	SERVER-MYSQL Oracle MySQL user enumeration attempt (1:24908)	4,632
71	SQL generic sql insert injection atttempt - POST parameter (1:15875)	4,606
72	BOTNET-CNC Trojan.Zeus P2P outbound communication attempt (1:22048)	4,499

No	Message	Jumlah
73	MALWARE-CNC Win.Trojan.Jorik variant outbound connection (1:20756)	4,409
74	MALWARE-CNC Possible host infection - excessive DNS queries for .eu (1:21544)	4,362
75	SCAN sqlmap SQL injection scan attempt (1:19779)	4,219
76	MALWARE-CNC Possible Zeus User-Agent - Mozilla (1:16442)	3,778
77	SQL ftp attempt (1:1057)	3,742
78	BLACKLIST User-Agent known malicious user agent BOT/0.1 (1:21925)	3,722
79	MALWARE-BACKDOOR radmin 3.0 runtime detection - login & remote control (1:12376)	3,614
80	MALWARE-CNC Trojan.DelfInject.gen!X outbound connection (1:19912)	3,490
81	BOTNET-CNC Torpig bot sinkhole server DNS lookup attempt (1:16693)	3,289
82	MALWARE-BACKDOOR netthief runtime detection (1:7760)	3,210
83	INDICATOR-OBFUSCATION Potential obfuscated javascript eval unescape attack attempt (1:15363)	3,110
84	SERVER-ORACLE BEA WebLogic Server Plug-ins Certificate overflow attempt (1:16606)	3,081
85	SQL version overflow attempt (1:2050)	3,046

No	Message	Jumlah
86	INDICATOR-COMPROMISE id check returned userid (1:1882)	3,022
87	SERVER-MSSQL heap-based overflow attempt (1:4989)	2,855
88	BOTNET-CNC W32.Dofoil variant outbound connectivity check (1:21312)	2,794
89	BLACKLIST DNS request for known malware domain jebena.ananikolic.su - Malware.HPsus/Palevo-B (1:24034)	2,761
90	SERVER-MSSQL sp_oacreate vulnerable function attempt (1:8497)	2,255
91	EXPLOIT-KIT RedKit Repeated Exploit Request Pattern (1:23218)	2,026
92	BOTNET-CNC Palevo bot DNS request for C&C attempt (1:16297)	1,756
93	BOTNET-CNC Palevo bot DNS request attempt (1:16298)	1,753
94	SERVER-IIS cmd.exe access (1:1002)	1,702
95	PUA-ADWARE Adware download accelerator plus runtime detection - download files (1:5904)	1,541
96	MALWARE-CNC ZeroAccess Clickserver callback (1:25054)	1,443
97	MALWARE-CNC Trojan.Kuluoz variant outbound connection (1:23244)	1,340
98	SERVER-MSSQL sp_oacreate unicode vulnerable function attempt (1:8496)	1,304

No	Message	Jumlah
99	MALWARE-CNC Win.Trojan.Yoddos.A outbound indicator (1:19769)	1,260
100	WEB-PHP Wordpress timthumb.php theme remote file include attack attempt (1:19653)	1,259

5.6.2 Agregasi Data Berdasarkan Bulan

Berdasarkan data kumulatif bulanan, tabel 5.4 menampilkan hasilnya

Tabel 5.6 Kumulatif Bulanan

Bulan	Jumlah
Januari	1,866,768.00
Februari	1,713,817.00
Maret	9,561,303.00
April	8,860,080.00
Mei	5,478,577.00
Juni	3,148,029.00
Juli	3,786,778.00
Agustus	1,988,865.00
September	2,459,626.00
Oktober	3,019,035.00

5.6.3 Agregasi Data Berdasarkan Data Harian

Agregasi data harian perlu untuk melihat tren kecenderungan serangan pada tiap harinya. Agregasi data harian pada buku ini tidak ditampilkan untuk alasan privasi. Sedangkan grafik tetap ditampillkan pada bab 6.

5.6.3 Agregasi Data Berdasarkan Negara Tujuan Serangan

Berdasarkan negara tujuan serangan, tabel 5.7 adalah daftar 100 negara tujuan serangan beserta jumlah serangan yang dihasilkan. Untuk melihat daftar lengkap, lihat Lampiran B

Tabel 5.7 100 Negara Tujuan Serangan Terbanyak

CountryName	Count
Indonesia	18,780,842
United States	8,579,014
China	1,612,341
Japan	1,328,457
India	1,004,882
Canada	918,522
Taiwan	769,083
Germany	542,668
Romania	498,634
Thailand	463,000
Russia	417,791
Brazil	355,576
France	351,310
Italy	339,985
United Kingdom	333,675
Sweden	326,917
Australia	275,249
Republic of Korea	248,924
Singapore	239,149
Hong Kong	224,516

CountryName	Count
Argentina	222,696
Bulgaria	214,616
Spain	214,167
Philippines	213,301
Netherlands	206,811
Poland	202,004
Venezuela	196,042
Ukraine	192,942
Malaysia	167,875
Vietnam	164,360
Turkey	131,113
Hungary	124,566
Israel	116,003
Colombia	114,534
Chile	97,814
Serbia	92,039
Portugal	89,010
Mexico	87,922
Sudan	78,954
Belgium	75,074
Iran	60,569
Denmark	57,687
Republic of Lithuania	55,925
Belarus	53,423
Bosnia and Herzegovina	52,790
Czech Republic	49,241

CountryName	Count
Kazakhstan	45,657
Pakistan	43,888
Switzerland	43,129
Saudi Arabia	41,697
Monaco	38,435
Norway	36,843
Georgia	36,777
New Zealand	35,981
Latvia	35,538
United Arab Emirates	29,386
Macedonia	27,467
Slovenia	26,277
South Africa	25,544
Croatia	24,132
Republic of Moldova	22,707
Morocco	21,309
Austria	19,886
Finland	18,980
Slovak Republic	16,728
Ireland	16,128
Greece	15,588
Panama	14,611
Bangladesh	13,546
Algeria	13,358
Uruguay	13,135
Armenia	13,073

CountryName	Count
Costa Rica	12,788
Trinidad and Tobago	11,565
Mongolia	11,535
Iraq	11,527
Estonia	11,372
Ecuador	8,537
Puerto Rico	8,223
Bahamas	6,962
Albania	6,399
Egypt	6,205
Tunisia	6,110
Montenegro	6,008
Nigeria	5,972
Qatar	5,827
Peru	5,662
Kyrgyzstan	5,539
Macao	5,050
Paraguay	4,966
Cyprus	4,764
Belize	4,414
Azerbaijan	4,355
Sri Lanka	4,165
Jamaica	3,864
Cambodia	3,666
Malta	3,420
Angola	3,397

CountryName	Count
Hashemite Kingdom of Jordan	3,144
Bolivia	3,045

5.6.4 Agregasi Data Berdasarkan Negara Penyerang

Berdasarkan negara penyerang, tabel 5.8 adalah daftar 100 negara penyerang beserta jumlah serangan yang dihasilkan. Untuk melihat daftar lengkap, lihat Lampiran C

Tabel 5.8 100 Negara Penyerang Terbanyak

CountryName	Count
Indonesia	27,759,147
China	7,627,189
Argentina	1,805,874
United States	1,090,489
France	700,930
Brazil	403,888
Russia	324,434
Netherlands	240,119
Taiwan	229,343
India	165,218
Canada	133,553
Germany	104,081
Vietnam	101,432
Hong Kong	88,699
Thailand	82,189
Japan	79,218
Mexico	73,883

CountryName	Count
Singapore	69,055
Ukraine	58,389
Republic of Korea	54,602
Philippines	54,509
Republic of Lithuania	49,653
Malaysia	43,961
Australia	41,967
United Kingdom	37,135
Israel	33,676
Turkey	32,432
Spain	30,334
Egypt	25,990
Italy	25,294
Estonia	24,122
Algeria	24,106
Chile	19,718
Romania	16,673
Bulgaria	15,876
Poland	13,464
Venezuela	13,306
Pakistan	12,021
Latvia	10,694
Sweden	10,640
Saudi Arabia	9,673
Ireland	8,476
Belgium	8,319

CountryName	Count
null	7,813
Morocco	6,851
New Zealand	5,723
United Arab Emirates	5,360
Switzerland	4,932
Hashemite Kingdom of Jordan	4,742
Iran	4,563
Denmark	4,232
Colombia	3,923
South Africa	3,531
Bahrain	3,287
Portugal	3,147
Ecuador	3,140
Dominican Republic	2,963
Albania	2,917
Serbia	2,718
Hungary	2,498
Greece	2,471
Bangladesh	2,269
Sri Lanka	2,202
Republic of Moldova	1,990
Peru	1,889
Cambodia	1,862
Austria	1,762
Paraguay	1,724
Kazakhstan	1,620

CountryName	Count
Czech Republic	1,605
Bosnia and Herzegovina	1,600
Norway	1,574
Tunisia	1,540
Palestine	1,475
Tanzania	1,392
Belarus	1,372
Belize	1,351
Guam	1,345
Luxembourg	1,333
Nigeria	1,128
Finland	1,094
Nepal	1,085
Slovak Republic	967
Qatar	861
Iraq	781
Maldives	766
Bolivia	748
Armenia	730
Kuwait	727
Uruguay	688
Macedonia	677
Slovenia	674
Lebanon	670
Azerbaijan	635
Syria	623

CountryName	Count
Croatia	532
Myanmar [Burma]	521
Senegal	509
Georgia	460
Kenya	388

5.6.5 Agregasi Data Berdasarkan Prioritas Serangan

SNORT memiliki penentuan prioritas serangan, apakah serangan itu memiliki prioritas tinggi, sedang maupun rendah. Jenis prioritas ditentukan oleh SNORT sehingga dalam data mentah yang ada dapat dilakukan agregasi. Tabel 5.9 menjelaskan mengenai prioritas serangan

Tabel 5.9 Prioritas Serangan

Priority	Jumlah
high	34016728
medium	7508248
low	357902

5.6.6 Agregasi Data Berdasarkan Klasifikasi Jenis Serangan dari SNORT Rule

SNORT juga memiliki klasifikasi tersendiri mengenai jenis serangan yang ada sehingga dalam data ini SNORT menyediakan jenis klasifikasi. Adapun data agregat mengenai klasifikasi jenis serangan terdapat pada tabel 5.10.

Tabel 5.10 Klasifikasi Jenis Serangan

Klasifikasi	Jumlah
A Network Trojan was Detected	19924654
Attempted User Privilege Gain	8578937
Misc Attack	5023353
Attempted Administrator Privilege Gain	4988185
An Attempted Login Using a Suspicious Username was Detected	2249333
Misc Activity	350457
Attempted Denial of Service	215061
Unsuccessful User Privilege Gain	201267
Web Application Attack	200750
Executabel Code was Detected	104432
Potential Corporate Policy Violation	16803
Access to a Potentially Vulnerable Web Application	9452
Generic Protocol Command Decode	7445
Attempted Information Leak	5443
Potentially Bad Traffic	3915
A Suspicious Filename was Detected	1086
Successful User Privilege Gain	1032
Successful Administrator Privilege Gain	661
Detection of a Denial of Service Attack	506
Information Leak	79
Attempt to Login By a Default Username and Password	20
http://www.agenbola.com/	7

5.6.7 Agregasi Data Berdasarkan IP Penyerang

Tabel 5.11 menampilkan 10 IP penyerang terbanyak beserta jumlah. Karena alasan kerahasiaan, maka IP tidak ditampilkan. Terlihat bahwa ada beberapa IP yang melakukan serangan lebih dari 100 ribu serangan.

Tabel 5.11 IP Penyerang Beserta Jumlah Serangan

Kode IP	Jumlah Serangan
S1	2415330
S2	2006511
S3	1152545
S4	1103380
S5	974552
S6	861201
S7	859691
S8	809819
S9	692939
S10	679775

5.6.8 Agregasi Data Berdasarkan IP Tujuan Serangan

Tabel 5.12 menampilkan 10 IP target terbanyak beserta jumlah. Karena alasan kerahasiaan, maka IP tidak ditampilkan. Terlihat bahwa ada terdapat beberapa IP yang mendapatkan serangan lebih dari 100 ribu.

Tabel 5.12 IP yang Diserang Beserta Jumlahnya

Kode IP	Jumlah
D1	242407
D2	140741
D3	140288
D4	137568
D5	131688
D6	127032
D7	123610
D8	119966
D9	102212
D10	93722

5.7 Visualisasi Data

Visualisasi data dilakukan dengan mengambil data agregat dari hasil agregasi pada sub-bab 5.5. Hasil pada visualisasi data dapat dilihat pada sub-bab 6.1

“Halaman ini sengaja dikosongkan”

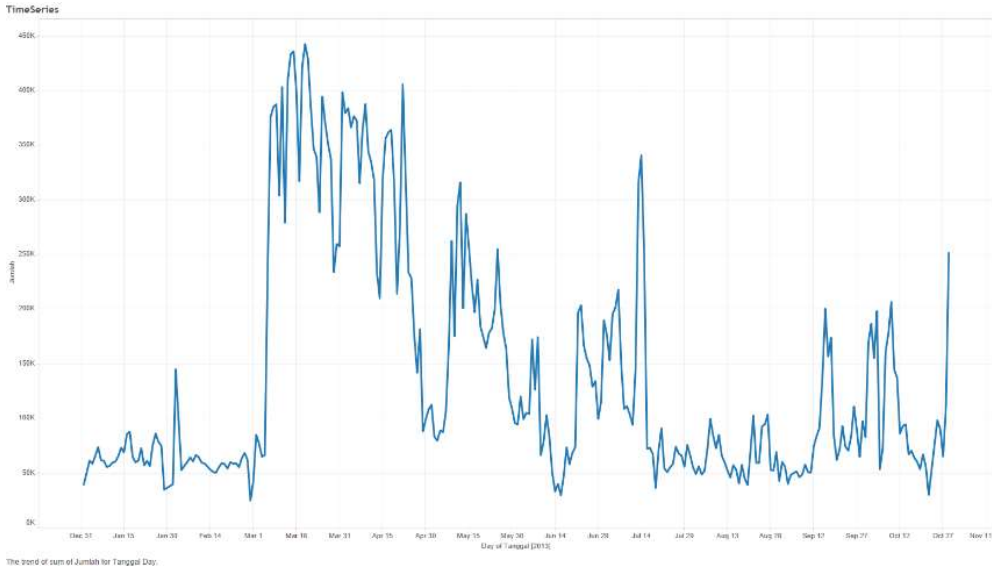
BAB VI
HASIL DAN ANALISA

Bab ini akan menjelaskan mengenai hasil dari agregasi data dan juga analisa data yang ada.

6.1 Analisa Visualisasi dan Agregasi Data

6.1.1 Timeseries

Gambar 6.1 merupakan grafik serangan perhari. Terlihat bahwa pada bulan Maret tercatat serangan tertinggi sepanjang bulan Januari hingga Oktober. Serangan tertinggi mencapai puncaknya pada tanggal 19 Maret 2013. Dapat dilihat bahwa jumlah serangan bervariasi setiap harinya.



Gambar 6.1 Timeseries Dari Grafik Serangan Perhari

6.1.2 Visualisasi Peta Negara Penyerang

Gambar 6.2 menampilkan gambar negara penyerang. Warna mengindikasikan jumlah serangan. Warna hijau menandakan jumlah serangan cukup sedikit (1 hingga 6.270 ribu serangan),

kuning menengah (6.270 ribu-18 juta) dan warna merah jumlah serangan tinggi (>18 juta).

Gambar 6.2 Peta Negara Penyerang

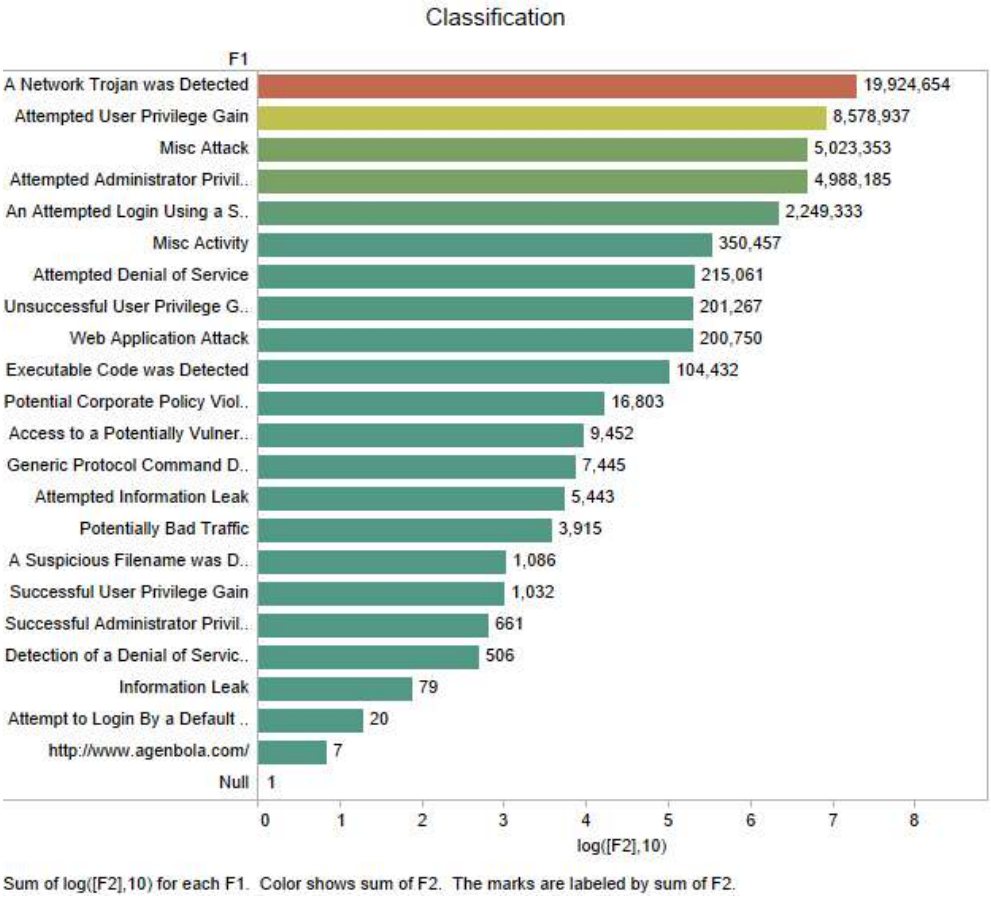
6.1.3 Visualisasi Peta Negara Tujuan

Gambar 6.3 menampilkan gambar negara tujuan. Warna mengindikasikan jumlah serangan. Warna hijau menandakan jumlah serangan cukup sedikit (1 – 4.680 ribu serangan), kuning menengah (4 juta hinga 9 juta) dan warna merah jumlah serangan tinggi (> 14 juta).

Gambar 6.3 Peta Negara Tujuan Serangan

6.1.4 Diagram Batang Klasifikasi Serangan

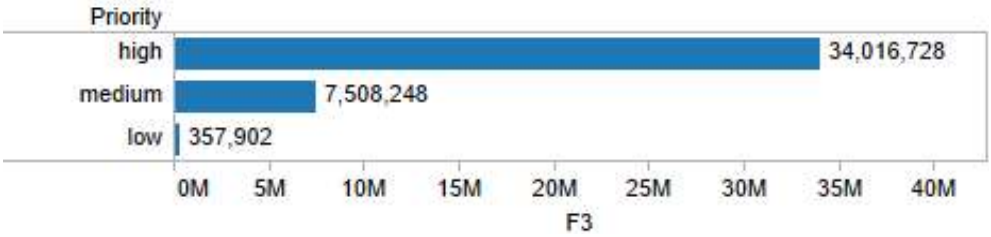
Pada gambar 6.4 menampilkan diagram batang dari masing-masing klasifikasi jenis serangan dari SNORT Rule. Panjang batang merupakan hasil dari log10 jumlah klasifikasi. Warna pada diagram batang mengindikasikan jumlah intensitas jumlah serangan. Serangan tertinggi ada pada A Network Trojan was Detected.



Gambar 6.4 Klasifikasi Serangan

6.1.5 Diagram Lingkar Prioritas Serangan

Gambar 6.5 menunjukkan jumlah prioritas serangan. Jumlah serangan tertinggi pada priority high dengan jumlah 34 juta serangan, sedangkan terendah pada priority low dengan hanya 300 ribu serangan.

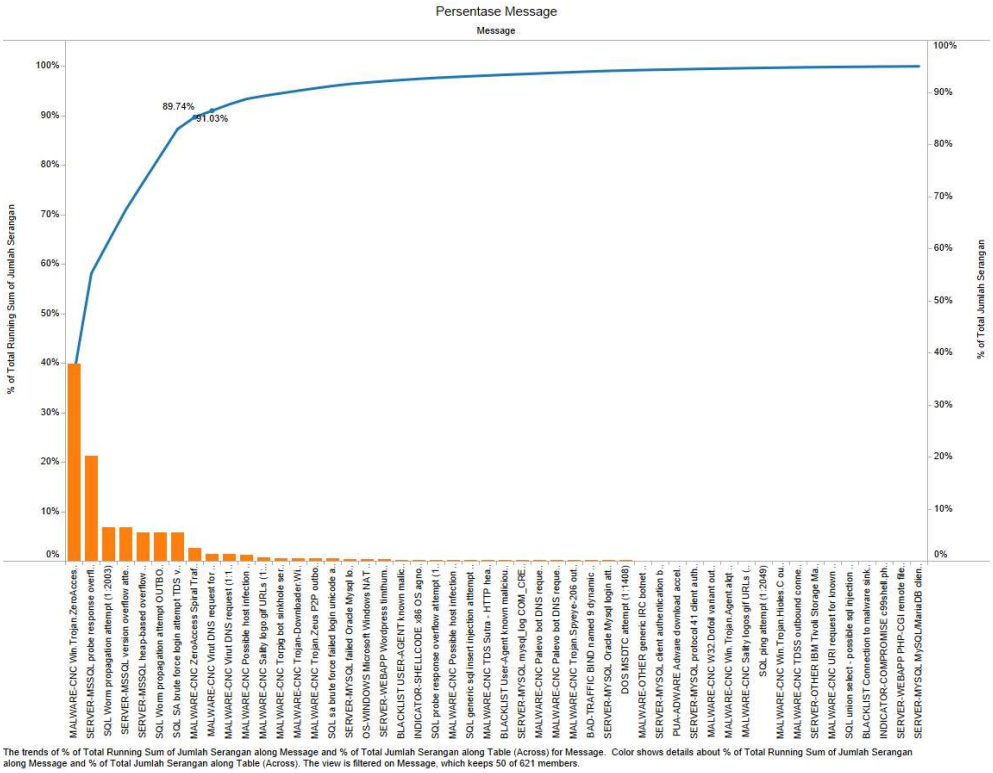


Gambar 6.5 Diagram Batang Prioritas Serangan

6.1.7 Jenis Message

Gambar 6.5 dan 6.6 menunjukkan persentase kumulatif dari masing-masing jenis message. Warna menunjukkan jenis-jenis serangan. Dari gambar 6.6 dapat terlihat bahwa lebih dari 50% serangan didominasi **hanya** oleh dua jenis serangan, yaitu dengan SNORT Rule 1:23493 dan 1:2329. Pada 90% serangan, **hanya 8** jenis serangan yang mendominasi seperti pada tabel 6.1

Gambar 6. 6 Diagram Batang Persebaran Jenis Malware



Gambar 6.7 Diagram Jenis Message. Terlihat Bahwa Hanya Beberapa Jenis Serangan yang Mendominasi

Tabel 6.1, 8 Malware yang Mendominasi 90% Serangan Internet di Indonesia

Rule	Message	Jumlah Serangan	Persentase	Kumulatif
123493	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication (1:23493)	15776139	37.67%	37.67%
12329	SERVER-MSSQL probe response overflow attempt (1:2329)	8416882	20.10%	57.76%

Rule	Message	Jumlah Serangan	Persentase	Kumulatif
12003	SQL Worm propagation attempt (1:2003)	2695211	6.44%	64.20%
12050	SERVER-MSSQL version overflow attempt (1:2050)	2662901	6.36%	70.56%
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)	2275018	5.43%	75.99%
12004	SQL Worm propagation attempt OUTBOUND (1:2004)	2250726	5.37%	81.36%
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)	2249253	5.37%	86.73%
125471	MALWARE-CNC ZeroAccess Spiral Traffic (1:25471)	1003710	2.40%	89.13%

Hal ini dapat disimpulkan bahwa serangan internet di Indonesia didominasi oleh dua jenis, yaitu Malware CNC Trojan Zero Access dan SQL Injection dengan berbagai variasinya.

Berdasarkan Pearce d.k.k. [13] ZeroAccess memiliki banyak bentuk sejak kemunculannya pada tahun 2009. Pearce juga mengatakan bahwa pada tahun 2013 populasinya lebih dari 1.9 juta serangan setiap hari pada Agustus 2013. Berdasarkan data dari Symantec [18], ZeroAccess dijual US$60.000 hingga US$120.000 pertahun dengan fitur yang lebih kaya. Lalu, ZeroAcces juga digunakan sebagai *Bitcoin Miner* yang menguntungkan sang penyerang. Selain itu, juga digunakan sebagai *click fraud* untuk melakukan unduhan pada iklan daring untuk menguntungkan penyerang. [18]

Selain itu, serangan yang mendominasi juga adalah serangan SQL Injection. Serangan ini memiliki berbagai varian,

dibedakan dari jenis klien dan juga jenis serangan. Pada tabel 6.1 jenis serangan didominasi oleh overflow dan juga bruteforce.

6.1.8 Analisa IP Penyerang

Untuk mengetahui mengapa terdapat IP yang memiliki jumlah serangan yang sangat tinggi, maka perlu untuk melihat jenis dan masing-masing jumlah. Dari 10 IP yang telah diidentifikasi, terdapat 8 IP yang memiliki kecenderungan menyerang hanya dengan jenis-jenis serangan tertentu dan jumlahnya cukup banyak. Hal ini diasumsikan bahwa memang IP tersebut merupakan IP yang khusus digunakan untuk melakukan serangan.

IP penyerang yang perlu diselidiki lebih lanjut memiliki ciri sebagai berikut :

- Memiliki jumlah serangan yang besar
- Memiliki varian jenis serangan yang sejenis dan tiap jenis memiliki jumlah yang besar, dan/atau
- Memiliki satu varian jenis serangan yang sangat besar namun memiliki beberapa jenis serangan yang sangat kecil sehingga dapat dianggap sebagai *outlier*. *Outlier* dapat muncul akibat kesalahan pengidentifikasian rule maupun gangguan pada penyerang

Berdasarkan kriteria tersebut, maka IP yang perlu diwaspadai antara lain

Tabel 6.2 Analisa IP Penyerang

Kode IP	Jumlah Serangan	Macam Jenis Serangan	Keragaman	Status
S1	2415330	4	Sejenis	Waspada
S2	2006511	7	Sejenis	Waspada
S3	1152545	34	Beragam	

Kode IP	Jumlah Serangan	Macam Jenis Serangan	Keragaman	Status
S4	1103380	6	Sejenis	Waspada
S5	974552	41	Beragam	
S6	861201	6	Sejenis	Waspada
S7	859691	1	Sejenis	Waspada
S8	809819	5	Sejenis	Waspada
S9	692939	4	Sejenis	Waspada
S10	679775	4	Sejenis	Waspada

6.2 Analisa Frequent Itemset Mining

6.2.1 Hasil Apriori

Berikut adalah hasil Apriori dengan minimum support 70%. Terdapat 51 pattern yang ada dengan masing-masing pattern merupakan satu jenis rule. Rule yang ada tidak mengindikasikan hubungan antar rule.

Tabel 6.3 Hasil Apriori dengan Minimum Support 70%

Pattern	#SUP:	Persentase
12329	298	100
11408	298	100
13528	298	100
13543	298	100
113990	298	100
315734	298	100

Pattern	#SUP:	Persentase
13668	298	100
116302	298	100
116304	298	100
113357	298	100
113358	298	100
12003	298	100
12050	298	100
119653	298	100
116693	298	100
13273	298	100
121849	298	100
115875	297	99.66443
14990	297	99.66443
12049	297	99.66443
13456	295	98.99329
15903	295	98.99329
12338	294	98.65772
121846	292	97.98658
117322	290	97.31544
113513	289	96.97987
121459	280	93.95973
116707	280	93.95973
13667	278	93.28859
121312	277	92.95302
117294	276	92.61745
12004	276	92.61745
115436	274	91.94631

Pattern	#SUP:	Persentase
116606	274	91.94631
122048	262	87.91946
11057	246	82.55034
11002	240	80.53691
124255	236	79.19463
123493	236	79.19463
124908	236	79.19463
125476	235	78.85906
114008	232	77.85235
121593	225	75.50336
113514	222	74.49664
116297	218	73.15436
116298	217	72.81879
122063	215	72.14765
11776	214	71.81208
14989	210	70.4698
125471	209	70.13423

Pada Apriori dengan minimum support 100%, maka dapat dilihat hasilnya sebagai berikut

Tabel 6.4 Hasil Rule dengan Minimum Support 100% Beserta Penjelasannya

Rule	Message
12329	SERVER-MSSQL probe response overflow attempt (1:2329)
11408	DOS MSDTC attempt (1:1408)
13528	SERVER-MYSQL create function access attempt (1:3528)
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)
113990	SQL union select - possible sql injection attempt - GET parameter (1:13990)
315734	BAD-TRAFFIC BIND named 9 dynamic update message remote dos attempt (3:15734)
13668	SERVER-MYSQL client authentication bypass attempt (1:3668)
116302	MALWARE-CNC Virut DNS request for C&C (1:16302)
116304	MALWARE-CNC Virut DNS request (1:16304)
113357	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)
113358	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)
12003	SQL Worm propagation attempt (1:2003)
12050	SERVER-MSSQL version overflow attempt (1:2050)
119653	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt (1:19653)

Rule	Message
116693	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693)
13273	SQL sa brute force failed login unicode attempt (1:3273)
121849	MALWARE-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)

Pada tabel 6.4 dapat dilihat bahwa jenis serangan didominasi oleh SQL attack, DOS, Malware CNC jenis virut DNS dan TDS Sutra dan juga serangan pada Wordpress. Hal ini dapat disimpulkan bahwa serangan ini setiap harinya mendominasi pada sensor IDS yang dimiliki oleh Id-SIRTII/CC. Untuk itu, perlu adanya penanganan pada jenis serangan yang selalu muncul

6.2.3 Hasil FP-Max

Pada FP-Max dengan nilai minimum support 95%, maka terdapat beberapa rule yang selalu muncul pada tiap pattern. Terdapat 18 jenis rule yang selalu muncul setiap pattern. Terdapat sepuluh pattern yang berhasil muncul. Adapun 18 jenis rule dijelaskan pada tabel 6.5.

Tabel 6.5 Jenis Serangan yang Selalu Muncul pada Setiap Pattern pada Minimum Support 95%

Rule	Message
11408	DOS MSDTC attempt (1:1408)
12003	SQL Worm propagation attempt (1:2003)
12050	SERVER-MSSQL version overflow attempt (1:2050)
12329	SERVER-MSSQL probe response overflow attempt (1:2329)

Rule	Message
13273	SQL sa brute force failed login unicode attempt (1:3273)
13528	SERVER-MYSQL create function access attempt (1:3528)
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)
13668	SERVER-MYSQL client authentication bypass attempt (1:3668)
113357	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)
113358	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)
113990	SQL union select - possible sql injection attempt - GET parameter (1:13990)
11408	DOS MSDTC attempt (1:1408)
12003	SQL Worm propagation attempt (1:2003)
12050	SERVER-MSSQL version overflow attempt (1:2050)
12329	SERVER-MSSQL probe response overflow attempt (1:2329)
13273	SQL sa brute force failed login unicode attempt (1:3273)
13528	SERVER-MYSQL create function access attempt (1:3528)
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)
13668	SERVER-MYSQL client authentication bypass attempt (1:3668)
113357	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)

Rule	Message
113358	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)
113990	SQL union select - possible sql injection attempt - GET parameter (1:13990)
116302	MALWARE-CNC Virut DNS request for C&C (1:16302)
116304	MALWARE-CNC Virut DNS request (1:16304)
116693	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693)
119653	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt (1:19653)
121849	MALWARE-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)
315734	BAD-TRAFFIC BIND named 9 dynamic update message remote dos attempt (3:15734)
12049	SQL ping attempt (1:2049)

Pada 18 jenis serangan diatas, terdapat beberapa jenis serangan, yaitu SQL Attack, Bad Traffic, Malware Virut DNS, Server Attack dan DoS. Hasil ini masih tidak jauh berbeda dengan algoritma Apriori. Pada DoS dengan rule 1:1408, berdasarkan SNORT Rule jenis ini melakukan serangan pada SQL Server sehingga kemungkinan memiliki keterkaitan pada SQL Attack.

Untuk dapat memudahkan analisis, maka rule yang selalu ada pada tiap pattern dihapus untuk mendapatkan pattern. Berikut adalah pattern yang sudah optimal.

Pattern 1

Tabel 6.6 Pattern 1 FP-Max Minimum Support 95%

Rule	Message
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)
113513	SQL generic sql insert injection atttempt - GET parameter (1:13513)

Pada pattern 1 ini, terdapat 18+ 4 rule yang mana didominasi oleh SQL Atack, kecuali pada rule 1:2338 yang menyerang pada server FTP.

Pattern 2

Tabel 6.7 Pattern 2 FP-Max Minimum Support 95%

Rule	Message
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)
113513	SQL generic sql insert injection atttempt - GET parameter (1:13513)

Pada pattern 2 ini mirip dengan pattern sebelumnya, namun terdapat rule 1:5903 yang merupakan adware. Serangan ini masih didominasi oleh SQL Attack

Pattern 3

Tabel 6.8 Pattern 3 FP-Max Minimum Support 95%

Rule	Message
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
13456	SERVER-MYSQL 4.0 root login attempt (1:3456)
113513	SQL generic sql insert injection atttempt - GET parameter (1:13513)

Pada pattern 3 serangan didominasi seluruhnya oleh SQL Attack.

Pattern 4

Tabel 6.9 Pattern 4 FP-Max Minimum Support 95%

Rule	Message
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)
121846	MALWARE-CNC TDS Sutra - request in.cgi (1:21846)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 4 serangan mulai beragam. Terdapat SQL Attack, serangan FTP, serangan dengan malware TDS Sutra dan juga exploit.

Pattern 5

Tabel 6.10 Pattern 5 FP-Max Minimum Support 95%

Rule	Message
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 5 serangan mulai beragam. Terdapat SQL Attack, serangan FTP, serangan adware dan juga exploit.

Pattern 6

Tabel 6.11 Pattern 6 FP-Max Minimum Support 95%

Rule	Message
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 6 terdapat berbagai serangan seperti SQL Attack, serangan FTP ,dan juga exploit.

Pattern 7

Tabel 6.12 Pattern 7 FP-Max Minimum Support 95%

Rule	Message
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
13456	SERVER-MYSQL 4.0 root login attempt (1:3456)
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 7 memiliki kemiripan dengan pattern 6, yaitu terdapat berbagai serangan seperti SQL Attack, serangan FTP ,dan juga exploit. Perbedaannya ada pada jenis SQL attack yang dijalankan

Pattern 8

Tabel 6.13 Pattern 8 FP-Max Minimum Support 95%

Rule	Message
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 8 memiliki kemiripan dengan pattern 6 dan 7, yaitu terdapat berbagai serangan seperti SQL Attack, serangan FTP ,dan juga exploit. Perbedaannya ada pada jenis SQL attack yang dijalankan

Pattern 9

Tabel 6.14 Pattern 9 FP-Max Minimum Support 95%

Rule	Message
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
13456	SERVER-MYSQL 4.0 root login attempt (1:3456)
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)

Pada pattern 9 memiliki kemiripan dengan pattern 5, yaitu terdapat berbagai serangan seperti SQL Attack dan serangan pada FTP. Perbedaan ada pada jenis SQL attack

Pattern 10

Tabel 6.15 Pattern 10 FP-Max Minimum Support 95%

Rule	**Message**
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)
13456	SERVER-MYSQL 4.0 root login attempt (1:3456)
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)

Rule	Message
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)
121846	MALWARE-CNC TDS Sutra - request in.cgi (1:21846)

Pattern 10 merupakan kumpulan semua rule yang ada pada jenis-jenis rule yang ada dari pattern 1-9. Sehingga dapat disimpulkan dengan minimum support 95% jenis-jenis yang ada adalah SQL attack, Adware, TDS Sutra, DoS, serangan pada Wordpress dan FTP server attack.

Pada pattern 99%, maka patternnya adalah sebagai berikut

Tabel 6.16 Pattern FP-Max Minimum Support 99%

Rule	Message
11408	DOS MSDTC attempt (1:1408)
12003	SQL Worm propagation attempt (1:2003)
12050	SERVER-MSSQL version overflow attempt (1:2050)
12329	SERVER-MSSQL probe response overflow attempt (1:2329)
13273	SQL sa brute force failed login unicode attempt (1:3273)
13528	SERVER-MYSQL create function access attempt (1:3528)
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)
13668	SERVER-MYSQL client authentication bypass attempt (1:3668)
113357	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)

Rule	Message
113358	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)
113990	SQL union select - possible sql injection attempt - GET parameter (1:13990)
116302	MALWARE-CNC Virut DNS request for C&C (1:16302)
116304	MALWARE-CNC Virut DNS request (1:16304)
116693	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693)
119653	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt (1:19653)
121849	MALWARE-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)
315734	BAD-TRAFFIC BIND named 9 dynamic update message remote dos attempt (3:15734)
12049	SQL ping attempt (1:2049)
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)

Pada tabel 6.16, mayoritas serangan merupakan satu macam, yaitu SQL attack. Serangan ini memiliki kesamaan, yaitu menyerang database SQL. Terdapat beberapa serangan yang bukan SQL attack, yaitu dengan rule nomor 3:15734 dan 1:1408, 1:16304, 1:16693, 1:19653.

Untuk melihat apakah ada rule tersebut berasosiasi atau hanya kebetulan muncul secara bersamaan, maka perlu untuk melihat database SNORT Rule. SNORT memiliki dokumentasi yang cukup lengkap. Pada rule dengan nomor 1:1408, serangan tersebut memiliki dampak terhadap SQL Server yang

terdistribusi sehingga dapat disimpulkan bahwa rule ini memiliki asosiasi dengan SQL Injection lainnya.

Selain itu, terdapat worm yang menyerang pada sistem operasi Windows seperti pada rule 1:16693 . Worm pada rule ini merupakan spyware yang akan memata-matai setiap aktivitas pengguna.

Selain itu, terdapat juga serangan terhadap DNS, yaitu pada rule 3:15734 , 1:16302,1:16304, 1:16693 Rule 3:15734 merupakan jenis serangan DoS, 1:16304,1:16693 dan 1:16302 merupakan exploit pada monitored network, yang mana juga merupakan salah satu akibat dari serangan Virut DNS.

6.3 Analisa Hasil VIsualisasi dan Frequent Itemset Mining

Dari hasil sub-bab sebelumnya, maka dapat dilakukan perbandingan antara jenis serangan yang masuk dalam 90% jumlah serangan, rule yang masuk pada FP-Max dengan minimum support 95% dan minimum support 99%.

Pada tabel 6.17 dibawah, merupakan hasil perbandingan antara 8 jenis serangan terbanyak dengan nilai support yang didapat dengan algoritma Apriori.

Tabel 6.17 Perbandingan Antara Message Terbanyak dengan Nilai Minimum Support

Rule	Message	Support	Jumlah Serangan
		%	
12003	SQL Worm propagation attempt (1:2003)	100.00%	2.695.211
12050	SERVER-MSSQL version overflow attempt (1:2050)	100.00%	2.250.726
12329	SERVER-MSSQL probe response overflow attempt (1:2329)	100.00%	2.662.901
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)	100.00%	8.416.882
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)	99.66%	2.249.253
12004	SQL Worm propagation attempt OUTBOUND (1:2004)	92.62%	2.275.018

Rule	Message	Support	Jumlah Serangan
		%	
123493	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication (1:23493)	79.19%	15.776.139
125471	MALWARE-CNC ZeroAccess Spiral Traffic (1:25471)	70.13%	1.003.710

Berdasarkan tabel 6.17, terjadi keanehan dimana jenis serangan Malware CNC yang merupakan jenis serangan terbesar hanya memiliki nilai support sebesar 70-80%. Seharusnya, dengan jumlah serangan yang cukup besar ia memiliki serangan yang cukup sering.

Berdasarkan hasil algoritma Apriori dengan minimum support 99%, ia memiliki kesamaan hasil dengan FP-Max 99%. Sehingga dapat ditarik kesimpulan bahwa hamper setiap hari, serangan yang terjadi adalah SQL Attack, DoS dan Malware TDS Sutra. Sedangkan jenis serangan terbanyak adalah Malware Zero Access dengan segala variannya.

Lalu, pada agregasi IP, terdapat beberapa 10 IP yang memiliki jumlah serangan yang besar. Pada 10 IP, 8 diantaranya memiliki jenis serangan yang sama sehingga dapat dicurigai bahwa IP tersebut merupakan mesin yang bekerja untuk melakukan serangan pada internet. Dari IP tersebut ditemukan bahwa jenis serangan yang dilancarkan adalah berjenis Malware Zero Access dan SQL Attack.

“halaman ini sengaja dibiarkan kosong”

LAMPIRAN A – Message

Lampiran ini berisikan informasi mengenai jenis serangan beserta jumlah kejadian yang terjadi sejak bulan Januari hingga Oktober. Tabel berisikan rule, nama jenis message, jumlah beserta presentase

Rule	Message	%	#
123493	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication (1:23493)	37.67%	15,776,139
12329	SERVER-MSSQL probe response overflow attempt (1:2329)	20.10%	8,416,882
12003	SQL Worm propagation attempt (1:2003)	6.44%	2,695,211
12050	SERVER-MSSQL version overflow attempt (1:2050)	6.36%	2,662,901
14990	SERVER-MSSQL heap-based overflow attempt (1:4990)	5.43%	2,275,018
12004	SQL Worm propagation attempt OUTBOUND (1:2004)	5.37%	2,250,726
13543	SQL SA brute force login attempt TDS v7/8 (1:3543)	5.37%	2,249,253
125471	MALWARE-CNC ZeroAccess Spiral Traffic (1:25471)	2.40%	1,003,710

Rule	Message	%	#
116302	MALWARE-CNC Virut DNS request for C&C (1:16302)	1.28%	536,264
116304	MALWARE-CNC Virut DNS request (1:16304)	1.28%	535,521
121545	MALWARE-CNC Possible host infection - excessive DNS queries for .ru (1:21545)	1.08%	453,291
124255	MALWARE-CNC Sality logo.gif URLs (1:24255)	0.62%	258,430
116693	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693)	0.53%	220,347
121227	MALWARE-CNC Trojan-Downloader.Win32.Bulknet.A outbound connection (1:21227)	0.51%	212,544
122048	MALWARE-CNC Trojan.Zeus P2P outbound communication (1:22048)	0.50%	210,158
13273	SQL sa brute force failed login unicode attempt (1:3273)	0.46%	193,250
113357	SERVER-MYSQL failed Oracle Mysql login attempt (1:13357)	0.40%	166,003
117294	OS-WINDOWS Microsoft Windows NAT Helper DNS query denial of service attempt (1:17294)	0.29%	121,177

Rule	Message	%	#
119653	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt (1:19653)	0.27%	115,072
119756	BLACKLIST USER-AGENT known malicious user-agent string Opera/8.89 - P2P-Worm.Win32.Palevo.ddm (1:19756)	0.23%	97,684
117322	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)	0.23%	94,932
12329	SQL probe response overflow attempt (1:2329)	0.20%	84,223
121546	MALWARE-CNC Possible host infection - excessive DNS queries for .cn (1:21546)	0.17%	70,953
113513	SQL generic sql insert injection atttempt - GET parameter (1:13513)	0.16%	65,755
121849	MALWARE-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)	0.15%	61,904
125476	BLACKLIST User-Agent known malicious user agent - User-Agent User-Agent (1:25476)	0.14%	60,439

Rule	Message	%	#
116707	SERVER-MYSQL mysql_log COM_CREATE_DB format string vulnerability exploit attempt (1:16707)	0.14%	57,332
116297	MALWARE-CNC Palevo bot DNS request for C&C (1:16297)	0.13%	56,083
116298	MALWARE-CNC Palevo bot DNS request (1:16298)	0.13%	56,058
120763	MALWARE-CNC Trojan.Spyeye-206 outbound connection (1:20763)	0.13%	55,789
315734	BAD-TRAFFIC BIND named 9 dynamic update message remote dos attempt (3:15734)	0.13%	53,883
113358	SERVER-MYSQL Oracle Mysql login attempt from unauthorized location (1:13358)	0.12%	48,706
11408	DOS MSDTC attempt (1:1408)	0.09%	38,689
119362	MALWARE-OTHER generic IRC botnet connection (1:19362)	0.07%	31,141
13668	SERVER-MYSQL client authentication bypass attempt (1:3668)	0.07%	28,637

Rule	Message	%	#
15903	PUA-ADWARE Adware download accelerator plus runtime detection - get ads (1:5903)	0.07%	28,292
13667	SERVER-MYSQL protocol 41 client authentication bypass attempt (1:3667)	0.07%	28,057
121312	MALWARE-CNC W32.Dofoil variant outbound connectivity check (1:21312)	0.06%	26,264
119484	MALWARE-CNC Win.Trojan.Agent.alqt variant outbound connection (1:19484)	0.06%	25,726
125809	MALWARE-CNC Sality logos.gif URLs (1:25809)	0.06%	23,605
12049	SQL ping attempt (1:2049)	0.05%	20,965
123391	MALWARE-CNC Win.Trojan.Hioles.C outbound connection (1:23391)	0.05%	20,524
121444	MALWARE-CNC TDSS outbound connection (1:21444)	0.05%	20,365
115436	SERVER-OTHER IBM Tivoli Storage Manager Express Backup counter heap corruption attempt (1:15436)	0.04%	17,148

Rule	Message	%	#
118938	MALWARE-CNC URI request for known malicious URI - ZBot (1:18938)	0.03%	14,485
113990	SQL union select - possible sql injection attempt - GET parameter (1:13990)	0.03%	13,431
125018	BLACKLIST Connection to malware sinkhole (1:25018)	0.03%	12,973
116627	INDICATOR-COMPROMISE c99shell.php command request - ls (1:16627)	0.03%	11,671
122063	SERVER-WEBAPP PHP-CGI remote file include attempt (1:22063)	0.02%	9,978
123115	SERVER-MYSQL MySQL/MariaDB client authentication bypass attempt (1:23115)	0.02%	9,424
117344	INDICATOR-SHELLCODE x86 OS agnostic xor dword decoder (1:17344)	0.02%	9,042
121846	MALWARE-CNC TDS Sutra - request in.cgi (1:21846)	0.02%	8,741
116302	BOTNET-CNC Virut DNS request for C&C attempt (1:16302)	0.02%	8,369

Rule	Message	%	#
124211	MALWARE-CNC RAT update protocol connection (1:24211)	0.02%	8,249
123972	MALWARE-CNC Trojan.Zbot variant outbound connection (1:23972)	0.02%	8,212
13528	SERVER-MYSQL create function access attempt (1:3528)	0.02%	8,050
1688	SQL sa login failed (1:688)	0.02%	8,017
121461	MALWARE-CNC Win.Trojan.DarkComet outbound connection - post infection (1:21461)	0.02%	7,444
121632	MALWARE-CNC Trojan.Ransom variant outbound connection (1:21632)	0.02%	7,407
113713	DELETED-MYSQL yaSSL SSLv2 Client Hello Message Challenge Buffer Overflow attempt (1:13713)	0.02%	7,338
13456	SERVER-MYSQL 4.0 root login attempt (1:3456)	0.02%	6,812
124439	BLACKLIST User-Agent known malicious user agent - Go http package (1:24439)	0.02%	6,649

Rule	Message	%	#
116431	SQL generic sql with comments injection attempt - GET parameter (1:16431)	0.01%	5,704
120630	MALWARE-CNC Win.Trojan.Winnti.A contact to cnc server (1:20630)	0.01%	5,596
12338	PROTOCOL-FTP LIST buffer overflow attempt (1:2338)	0.01%	5,590
116304	BOTNET-CNC Virut DNS request attempt (1:16304)	0.01%	5,383
317429	WEB-MISC Microsoft ASP.NET information disclosure attempt (3:17429)	0.01%	5,371
121593	MALWARE-CNC Trojan.Dropper-23836 outbound connection (1:21593)	0.01%	5,221
121459	MALWARE-TOOLS Havij advanced SQL injection tool user-agent string (1:21459)	0.01%	4,855
124908	SERVER-MYSQL Oracle MySQL user enumeration attempt (1:24908)	0.01%	4,632
115875	SQL generic sql insert injection atttempt - POST parameter (1:15875)	0.01%	4,606

Rule	Message	%	#
122048	BOTNET-CNC Trojan.Zeus P2P outbound communication attempt (1:22048)	0.01%	4,499
120756	MALWARE-CNC Win.Trojan.Jorik variant outbound connection (1:20756)	0.01%	4,409
121544	MALWARE-CNC Possible host infection - excessive DNS queries for .eu (1:21544)	0.01%	4,362
119779	SCAN sqlmap SQL injection scan attempt (1:19779)	0.01%	4,219
116442	MALWARE-CNC Possible Zeus User-Agent - Mozilla (1:16442)	0.01%	3,778
11057	SQL ftp attempt (1:1057)	0.01%	3,742
121925	BLACKLIST User-Agent known malicious user agent BOT/0.1 (1:21925)	0.01%	3,722
112376	MALWARE-BACKDOOR radmin 3.0 runtime detection - login & remote control (1:12376)	0.01%	3,614
119912	MALWARE-CNC Trojan.DelfInject.gen!X outbound connection (1:19912)	0.01%	3,490

Rule	Message	%	#
116693	BOTNET-CNC Torpig bot sinkhole server DNS lookup attempt (1:16693)	0.01%	3,289
17760	MALWARE-BACKDOOR netthief runtime detection (1:7760)	0.01%	3,210
115363	INDICATOR-OBFUSCATION Potential obfuscated javascript eval unescape attack attempt (1:15363)	0.01%	3,110
116606	SERVER-ORACLE BEA WebLogic Server Plug-ins Certificate overflow attempt (1:16606)	0.01%	3,081
12050	SQL version overflow attempt (1:2050)	0.01%	3,046
11882	INDICATOR-COMPROMISE id check returned userid (1:1882)	0.01%	3,022
14989	SERVER-MSSQL heap-based overflow attempt (1:4989)	0.01%	2,855
121312	BOTNET-CNC W32.Dofoil variant outbound connectivity check (1:21312)	0.01%	2,794
124034	BLACKLIST DNS request for known malware domain jebena.ananikolic.su -	0.01%	2,761

Rule	Message	%	#
	Malware.HPsus/Palevo-B (1:24034)		
18497	SERVER-MSSQL sp_oacreate vulnerable function attempt (1:8497)	0.01%	2,255
123218	EXPLOIT-KIT RedKit Repeated Exploit Request Pattern (1:23218)	0.00%	2,026
116297	BOTNET-CNC Palevo bot DNS request for C&C attempt (1:16297)	0.00%	1,756
116298	BOTNET-CNC Palevo bot DNS request attempt (1:16298)	0.00%	1,753
11002	SERVER-IIS cmd.exe access (1:1002)	0.00%	1,702
15904	PUA-ADWARE Adware download accelerator plus runtime detection - download files (1:5904)	0.00%	1,541
125054	MALWARE-CNC ZeroAccess Clickserver callback (1:25054)	0.00%	1,443
123244	MALWARE-CNC Trojan.Kuluoz variant outbound connection (1:23244)	0.00%	1,340
18496	SERVER-MSSQL sp_oacreate unicode vulnerable function attempt (1:8496)	0.00%	1,304

Rule	Message	%	#
119769	MALWARE-CNC Win.Trojan.Yoddos.A outbound indicator (1:19769)	0.00%	1,260
119653	WEB-PHP Wordpress timthumb.php theme remote file include attack attempt (1:19653)	0.00%	1,259
113989	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation (1:13989)	0.00%	1,257
115165	MALWARE-CNC Pushdo client communication (1:15165)	0.00%	1,256
122033	MALWARE-CNC Apple OSX Flashback malware outbound connection (1:22033)	0.00%	1,219
121384	MALWARE-CNC Win.Trojan.Nuqel.Q host freewebs.com runtime traffic detected (1:21384)	0.00%	1,214
113357	POLICY failed Oracle Mysql login attempt (1:13357)	0.00%	1,195
115874	SQL union select - possible sql injection attempt - POST parameter (1:15874)	0.00%	1,112

Rule	Message	%	#
120763	BOTNET-CNC Trojan.Spyeye-206 outbound connection (1:20763)	0.00%	1,094
113514	SQL generic sql update injection attempt - GET parameter (1:13514)	0.00%	1,092
118939	MALWARE-CNC known command and control channel traffic (1:18939)	0.00%	1,080
117387	SERVER-APACHE Apache Tomcat allowLinking URIencoding directory traversal attempt (1:17387)	0.00%	1,076
114008	INDICATOR-OBFUSCATION large number of calls to concat function - possible sql injection obfuscation (1:14008)	0.00%	1,036
121860	EXPLOIT-KIT Phoenix exploit kit post-compromise behavior (1:21860)	0.00%	1,031
116495	MALWARE-CNC Rustock botnet variant outbound connection (1:16495)	0.00%	1,016
318431	WEB-CLIENT Firefox Acrobat Reader sqlite.dll	0.00%	WEB-CLIENT

Rule	Message	%	#
	dll-load exploit attempt (3:18431)		Firefox Acrobat Reader sqlite.dll dll-load exploit attempt (3:18431)
121269	MALWARE-CNC W32.Cycbot variant outbound connection (1:21269)	0.00%	962
117043	FILE-IDENTIFY Microsoft Windows PIF shortcut file download request (1:17043)	0.00%	909
121551	MALWARE-CNC Trojan.Kahn outbound connection (1:21551)	0.00%	890
121229	MALWARE-CNC Win.Trojan.Synljdos.A outbound connection (1:21229)	0.00%	883
118247	BLACKLIST USER-AGENT known malicious User-Agent ErrCode - W32/Fujacks.htm (1:18247)	0.00%	882

Rule	Message	%	#
115169	POLICY-SOCIAL XBOX Live Kerberos authentication request (1:15169)	0.00%	873
125783	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation (1:25783)	0.00%	867
114082	MALWARE-CNC Win.Trojan.agent.aarm variant outbound connection spread via spam (1:14082)	0.00%	816
123626	SERVER-IIS cmd.exe access (1:23626)	0.00%	786
125627	MALWARE-CNC Ranson File Encrypter outbound communication (1:25627)	0.00%	784
116622	INDICATOR-COMPROMISE c99shell.php command request - sql (1:16622)	0.00%	780
116628	INDICATOR-COMPROMISE c99shell.php command request - phpinfo (1:16628)	0.00%	751
125224	MALWARE-CNC Win.Trojan.ZeroAccess URI and Referer (1:25224)	0.00%	739

Rule	Message	%	#
125256	MALWARE-CNC Win.Worm.Gamarue outbound connection (1:25256)	0.00%	729
117407	FILE-IDENTIFY Microsoft Windows help file download request (1:17407)	0.00%	710
119175	BLACKLIST USER-AGENT known malicious User-Agent wget 3.0 (1:19175)	0.00%	697
124814	SNMP Samsung printer default community string (1:24814)	0.00%	672
121104	MALWARE-TOOLS slowhttptest DoS tool (1:21104)	0.00%	634
11776	SERVER-MYSQL show databases attempt (1:1776)	0.00%	614
112278	FILE-IDENTIFY Microsoft Media Player compressed skin download request (1:12278)	0.00%	609
124397	APP-DETECT Steam game URI handler (1:24397)	0.00%	606
123246	PUA-ADWARE Wajam Monitizer url outbound connection - post install (1:23246)	0.00%	605

Rule	Message	%	#
117546	FILE-IDENTIFY Microsoft Media Player compressed skin download request (1:17546)	0.00%	591
120232	MALWARE-CNC Win.Trojan.Cycbot outbound connection (1:20232)	0.00%	546
111264	SERVER-MSSQL Microsoft SQL Server 2000 Server hello buffer overflow attempt (1:11264)	0.00%	539
124577	BLACKLIST User-Agent known malicious user agent - MyApp (1:24577)	0.00%	538
125526	EXPLOIT-KIT Multiple Exploit Kit Payload detection - setup.exe (1:25526)	0.00%	538
121538	MALWARE-CNC W32.Dofoil variant outbound payload request (1:21538)	0.00%	534
121188	BLACKLIST User-Agent known malicious user-agent string API Guide test program (1:21188)	0.00%	533
1498	INDICATOR-COMPROMISE id check returned root (1:498)	0.00%	520

Rule	Message	%	#
121965	BLACKLIST USER-AGENT known malicious user agent VB WININET (1:21965)	0.00%	517
119779	SERVER-WEBAPP sqlmap SQL injection scan attempt (1:19779)	0.00%	510
113553	SERVER-OTHER Sybase SQL Anywhere Mobilink username string buffer overflow (1:13553)	0.00%	498
113902	SERVER-OTHER IBM Lotus Sametime multiplexer stack buffer overflow attempt (1:13902)	0.00%	489
121488	APP-DETECT User-Agent known user agent - GetRight (1:21488)	0.00%	478
123715	FILE-IDENTIFY Microsoft Office Access file magic detected (1:23715)	0.00%	468
12123	INDICATOR-COMPROMISE Microsoft cmd.exe banner (1:2123)	0.00%	462
122058	MALWARE-CNC Trojan.Kbot variant outbound connection (1:22058)	0.00%	441
121547	MALWARE-CNC Win.Trojan.Kazy variant	0.00%	438

Rule	Message	%	#
	outbound connection (1:21547)		
11385	SERVER-WEBAPP mod-plsql administration access (1:1385)	0.00%	436
116299	MALWARE-CNC Palevo bot DNS request (1:16299)	0.00%	434
116708	SERVER-MYSQL mysql_log COM_DROP_DB format string vulnerability exploit attempt (1:16708)	0.00%	381
113712	DELETED-MYSQL yaSSL SSLv2 Client Hello Message Session ID Buffer Overflow attempt (1:13712)	0.00%	379
115306	FILE-EXECUTABEL Portabel Executabel binary file magic detected (1:15306)	0.00%	371
115876	SQL generic sql update injection attempt - POST parameter (1:15876)	0.00%	363
11061	SQL xp_cmdshell attempt (1:1061)	0.00%	361
116621	INDICATOR-COMPROMISE c99shell.php command request - security (1:16621)	0.00%	360

Rule	Message	%	#
113358	POLICY Oracle Mysql login attempt from unauthorized location (1:13358)	0.00%	357
15903	SPYWARE-PUT Adware download accelerator plus runtime detection - get ads (1:5903)	0.00%	353
119998	POLICY-OTHER IP address discosure to advertisement sites attempt (1:19998)	0.00%	349
125652	MALWARE-CNC Win.Trojan.Kryptic variant outbound connection (1:25652)	0.00%	345
124334	BLACKLIST User-Agent known malicious user agent - IE9 (1:24334)	0.00%	340
112374	MALWARE-BACKDOOR radmin 3.0 runtime detection - initial connection (1:12374)	0.00%	326
116364	DOS IBM DB2 database server SQLSTT denial of service attempt (1:16364)	0.00%	325
117533	SERVER-APACHE Apache Struts Information Disclosure Attempt (1:17533)	0.00%	320

Rule	Message	%	#
18713	SERVER-WEBAPP cacti graph_image SQL injection attempt (1:8713)	0.00%	309
119164	MALWARE-CNC Win.Trojan.SpyEye outbound connection (1:19164)	0.00%	301
123701	FILE-IDENTIFY Microsoft SYmbolic LinK file magic detected (1:23701)	0.00%	274
117344	SHELLCODE x86 OS agnostic xor dword decoder (1:17344)	0.00%	269
113713	MYSQL yaSSL SSLv2 Client Hello Message Challenge Buffer Overflow attempt (1:13713)	0.00%	265
117564	SERVER-IIS WebDAV Request Directory Security Bypass attempt (1:17564)	0.00%	258
1887	SERVER-WEBAPP www-sql access (1:887)	0.00%	247
11292	INDICATOR-COMPROMISE directory listing (1:1292)	0.00%	239
318427	DELETED WEB-CLIENT Firefox Acrobat Reader ace.dll dll-load exploit attempt - DISABLED (3:18427)	0.00%	234

Rule	Message	%	#
113663	SERVER-MAIL Alt-N MDaemon IMAP Server FETCH command buffer overflow attempt (1:13663)	0.00%	225
11661	SERVER-IIS cmd32.exe access (1:1661)	0.00%	222
122064	SERVER-WEBAPP PHP-CGI command injection attempt (1:22064)	0.00%	222
119608	MALWARE-CNC Win.Trojan.Wisscmd.A outbound connection (1:19608)	0.00%	214
121632	BOTNET-CNC Trojan.Ransom variant outbound connection (1:21632)	0.00%	209
1861	SERVER-WEBAPP w3-msql access (1:861)	0.00%	206
117484	DNS squid proxy dns PTR record response denial of service attempt (1:17484)	0.00%	203
124861	EXPLOIT-KIT Blackholev2 landing page in an email (1:24861)	0.00%	199
116990	POLICY-SPAM nextmail.ru known spam email attempt (1:16990)	0.00%	199
11078	SQL counter.exe access (1:1078)	0.00%	196

Rule	Message	%	#
124632	BLACKLIST User-Agent known malicious user agent - 1 (1:24632)	0.00%	195
1052	BO_CLIENT_TRAFFIC_ DETECT (105:2)	0.00%	195
115306	FILE-IDENTIFY Portabel Executabel binary file magic detected (1:15306)	0.00%	195
118287	DELETED SPECIFIC-THREATS Apache Tomcat JK Web Server Connector long URL stack overflow attempt (1:18287)	0.00%	187
118944	MALWARE-CNC URI request for known malicious URI - Suspected Crimepack (1:18944)	0.00%	181
121475	BLACKLIST User-Agent known malicious user-agent string core-project (1:21475)	0.00%	180
118756	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows 7/Server 2008R2 (1:18756)	0.00%	175
116303	MALWARE-CNC Virut DNS request (1:16303)	0.00%	171
114086	MALWARE-CNC Adware.Win32.Agent.BM outbound connection 1 (1:14086)	0.00%	170

Rule	Message	%	#
119657	MALWARE-CNC FakeAV variant traffic (1:19657)	0.00%	167
19331	MALWARE-OTHER mydoom.m smtp propagation detection (1:9331)	0.00%	166
13668	MYSQL client authentication bypass attempt (1:3668)	0.00%	164
121418	MALWARE-CNC Trojan.FareIt outbound connection (1:21418)	0.00%	163
121849	BOTNET-CNC TDS Sutra - HTTP header redirecting to a SutraTDS (1:21849)	0.00%	159
13672	SERVER-MYSQL client overflow attempt (1:3672)	0.00%	159
119454	MALWARE-CNC Trojan.PWS.Win32.QQPass.IK outbound connection (1:19454)	0.00%	158
121525	MALWARE-CNC Trojan.Downloader variant outbound connection (1:21525)	0.00%	157
123115	SQL MySQL/MariaDB client authentication bypass attempt (1:23115)	0.00%	157
121591	BLACKLIST USER-AGENT known Adware	0.00%	156

Rule	Message	%	#
	user agent Gamevance tl_v (1:21591)		
318439	WEB-CLIENT Acrobat Reader IE plugin ace.dll dll-load exploit attempt (3:18439)	0.00%	154
120104	BLACKLIST User-Agent known malicious user-agent string - InfoBot (1:20104)	0.00%	150
12091	SERVER-IIS WEBDAV nessus safe scan attempt (1:2091)	0.00%	146
118612	SERVER-WEBAPP Oracle Java Web Server WebDAV Stack Buffer Overflow attempt (1:18612)	0.00%	144
113711	DELETED MYSQL yaSSL SSLv2 Client Hello Message Cipher Length Buffer Overflow attempt (1:13711)	0.00%	142
123058	MALWARE-OTHER NeoSploit Malvertising - URI Requested (1:23058)	0.00%	140
116615	INDICATOR-COMPROMISE c99shell.php command request - upload (1:16615)	0.00%	138
116008	OS-WINDOWS Multiple Products excessive HTTP	0.00%	137

Rule	Message	%	#
	304 Not Modified responses exploit attempt (1:16008)		
116356	SERVER-IIS multiple extension code execution attempt (1:16356)	0.00%	136
121092	MALWARE-TOOLS JavaScript LOIC attack (1:21092)	0.00%	135
13528	MYSQL create function access attempt (1:3528)	0.00%	134
1117	MALWARE-BACKDOOR Infector.1.x (1:117)	0.00%	130
313887	BAD-TRAFFIC dns root nameserver poisoning attempt (3:13887)	0.00%	125
113714	SERVER-MYSQL yaSSL SSLv3 Client Hello Message Cipher Specs Buffer Overflow attempt (1:13714)	0.00%	123
124566	MALWARE-CNC Win.Trojan.Jorik variant outbound connection (1:24566)	0.00%	122
313308	WEB-MISC Apache HTTP server auth_ldap logging function format string vulnerability (3:13308)	0.00%	122

Rule	Message	%	#
125323	EXPLOIT-KIT Cool Exploit Kit EOT file download (1:25323)	0.00%	114
116341	SERVER-OTHER IBM DB2 Database Server invalid data stream denial of service attempt (1:16341)	0.00%	111
115930	OS-WINDOWS Microsoft Windows SMB malformed process ID high field remote code execution attempt (1:15930)	0.00%	109
121278	BLACKLIST User-Agent known malicious user-agent string Google Bot (1:21278)	0.00%	107
17649	MALWARE-BACKDOOR minicom lite runtime detection - server-to-client (1:7649)	0.00%	105
124491	MALWARE-CNC Win.Trojan.Vundo redirection landing page pre-infection (1:24491)	0.00%	100
121926	SERVER-WEBAPP JCE Joomla module vulnerable directory traversal or malicious file upload attempt (1:21926)	0.00%	99
115436	EXPLOIT IBM Tivoli Storage Manager Express	0.00%	94

Rule	Message	%	#
	Backup counter heap corruption attempt (1:15436)		
125664	SERVER-OTHER MiniUPnPd SSDP request buffer overflow attempt (1:25664)	0.00%	94
123218	SPECIFIC-THREATS RedKit Repeated Exploit Request Pattern (1:23218)	0.00%	94
117339	INDICATOR-SHELLCODE x86 generic OS alpha numeric mixed case decoder (1:17339)	0.00%	93
123757	FILE-IDENTIFY Microsoft Windows CHM file magic detected (1:23757)	0.00%	90
1494	INDICATOR-COMPROMISE command completed (1:494)	0.00%	90
113593	DELETED MYSQL yaSSL SSL Hello Message Buffer Overflow attempt (1:13593)	0.00%	89
120827	SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt (1:20827)	0.00%	88
316415	WEB-CLIENT Microsoft DirectShow memory	0.00%	88

Rule	Message	%	#
	corruption attempt (3:16415)		
125568	EXPLOIT-KIT Blackhole Exploit Kit landing page retrieval (1:25568)	0.00%	87
124475	EXPLOIT-KIT Blackhole - Cookie Set (1:24475)	0.00%	83
1673	SQL sp_start_job - program execution (1:673)	0.00%	82
114087	MALWARE-CNC Adware.Win32.Agent.BM outbound connection 2 (1:14087)	0.00%	80
1686	SERVER-MSSQL xp_reg* - registry access (1:686)	0.00%	80
13542	SQL SA brute force login attempt (1:3542)	0.00%	80
11077	SQL queryhit.htm access (1:1077)	0.00%	79
120106	BLACKLIST User-Agent known malicious user-agent string - darkness (1:20106)	0.00%	78
121846	BOTNET-CNC TDS Sutra - request in.cgi (1:21846)	0.00%	77
315453	NETBIOS SMB replay attempt via NTLMSSP - overlapping encryption keys detected (3:15453)	0.00%	77

Rule	Message	%	#
113519	SERVER-OTHER Citrix MetaFrame IMA buffer overflow attempt (1:13519)	0.00%	76
11527	SERVER-WEBAPP basilix mysql.class access (1:1527)	0.00%	67
120756	BOTNET-CNC Win32.Jorik variant outbound connection (1:20756)	0.00%	66
116716	FILE-IMAGE Oracle Java Web Start Splashscreen PNG processing buffer overflow attempt (1:16716)	0.00%	66
117543	FILE-OFFICE Microsoft Office Excel Column record handling memory corruption attempt (1:17543)	0.00%	66
125043	EXPLOIT-KIT Blackholev2 url structure detected (1:25043)	0.00%	65
116982	POLICY-SPAM 64.com1.ru known spam email attempt (1:16982)	0.00%	64
13671	SERVER-MYSQL protocol 41 client overflow attempt (1:3671)	0.00%	64
125266	SERVER-OTHER Adobe ColdFusion Admin API	0.00%	63

Rule	Message	%	#
	arbitrary command execution attempt (1:25266)		
116214	DOS Squid Proxy invalid HTTP response code denial of service attempt (1:16214)	0.00%	62
124863	EXPLOIT-KIT Blackholev2 landing page in an email (1:24863)	0.00%	62
15801	PUA-TOOLBARS Trackware myway speedbar / mywebsearch toolbar runtime detection - track activity 1 (1:5801)	0.00%	62
12133	SERVER-IIS MS BizTalk server access (1:2133)	0.00%	62
115437	SERVER-OTHER IBM Tivoli Storage Manager Express Backup message length heap corruption attempt (1:15437)	0.00%	61
1683	SQL sp_password - password change (1:683)	0.00%	60
18361	MALWARE-BACKDOOR black curse 4.0 runtime detection - inverse init connection (1:8361)	0.00%	58
116809	MALWARE-CNC known command and control channel traffic (1:16809)	0.00%	58

Rule	Message	%	#
121492	EXPLOIT-KIT Blackhole landing page with specific structure - prototype catch (1:21492)	0.00%	56
116616	INDICATOR-COMPROMISE c99shell.php command request - about (1:16616)	0.00%	55
111319	MALWARE-BACKDOOR netwindow runtime detection - init connection request (1:11319)	0.00%	55
11871	SERVER-WEBAPP Oracle XSQLConfig.xml access (1:1871)	0.00%	55
117609	SERVER-WEBAPP Oracle Java Web Server WebDAV Stack Buffer Overflow attempt (1:17609)	0.00%	52
315850	EXPLOIT Remote Desktop orderType remote code execution attempt (3:15850)	0.00%	50
1687	SQL xp_cmdshell - program execution (1:687)	0.00%	50
1509	SERVER-WEBAPP PCCS mysql database admin tool access (1:509)	0.00%	49

Rule	Message	%	#
121686	EXPLOIT-KIT Bleeding Life exploit module call (1:21686)	0.00%	48
125780	SERVER-OTHER MiniUPnPd ExecuteSoapAction buffer overflow attempt (1:25780)	0.00%	46
121910	MALWARE-CNC Apple OSX Flashback malware user-agent (1:21910)	0.00%	45
121440	MALWARE-CNC Win.Trojan.Murofet variant outbound connection (1:21440)	0.00%	45
124442	BLACKLIST User-Agent known malicious user agent - Alerter COM (1:24442)	0.00%	44
12338	FTP LIST buffer overflow attempt (1:2338)	0.00%	44
323180	SMTP obfuscated header in PDF attachment (3:23180)	0.00%	44
125739	BLACKLIST DNS request for known malware domain facesystem.in (1:25739)	0.00%	43
116813	MALWARE-CNC known command and control channel traffic (1:16813)	0.00%	42

Rule	Message	%	#
123492	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication (1:23492)	0.00%	42
113791	INDICATOR-OBFUSCATION oversized cast statement - possible sql injection obfuscation (1:13791)	0.00%	41
15904	SPYWARE-PUT Adware download accelerator plus runtime detection - download files (1:5904)	0.00%	41
1220	MALWARE-BACKDOOR HideSource backdoor attempt (1:220)	0.00%	40
118464	SERVER-WEBAPP Adobe ColdFusion locale directory traversal attempt (1:18464)	0.00%	39
119779	WEB-MISC sqlmap SQL injection scan attempt (1:19779)	0.00%	39
318434	NETBIOS Acrobat Reader IE plugin ace.dll dll-load exploit attempt (3:18434)	0.00%	37
117322	SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder (1:17322)	0.00%	37
120105	BLACKLIST User-Agent known malicious user-	0.00%	36

Rule	Message	%	#
	agent string - IPHONE (1:20105)		
117294	DOS Microsoft Windows NAT Helper DNS query denial of service attempt (1:17294)	0.00%	36
121459	SPECIFIC-THREATS Havij advanced SQL injection tool user-agent string (1:21459)	0.00%	36
11387	SQL raiserror possible buffer overflow (1:1387)	0.00%	35
119123	MALWARE-CNC Dropper Win.Trojan.Cefyns.A outbound connection (1:19123)	0.00%	34
124441	BLACKLIST User-Agent known malicious user agent - Testing (1:24441)	0.00%	33
125820	EXPLOIT-KIT CritX Exploit Kit possible plugin detection attempt (1:25820)	0.00%	33
119623	BLACKLIST URI request for known malicious URI - vic.aspx?ver= (1:19623)	0.00%	32
117323	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder unescaped (1:17323)	0.00%	32

Rule	Message	%	#
123615	MALWARE-CNC ACAD.Medre.A outbound connection (1:23615)	0.00%	32
13690	SERVER-WEBAPP Nucleus CMS action.php itemid SQL injection (1:3690)	0.00%	32
125596	EXPLOIT-KIT Cool Exploit Kit EOT file download (1:25596)	0.00%	30
118431	FILE-PDF Acrobat Reader plugin sqlite.dll dll-load exploit attempt (1:18431)	0.00%	30
316320	WEB-CLIENT Adobe PNG empty sPLT exploit attempt (3:16320)	0.00%	30
119595	BLACKLIST EMAIL known malicious email string - You have received a Hallmark E-Card! (1:19595)	0.00%	29
318422	DELETED NETBIOS Firefox Acrobat Reader ace.dll dll-load exploit attempt - DISABLED (3:18422)	0.00%	29
123156	EXPLOIT-KIT URI Nuclear Pack exploit kit landing page (1:23156)	0.00%	29
121562	MALWARE-CNC Trojan.Bredolab variant	0.00%	29

Rule	Message	%	#
	outbound connection (1:21562)		
120679	MALWARE-CNC Win.Trojan.Syrutrk variant outbound connection (1:20679)	0.00%	29
115364	SERVER-OTHER Ganglia Meta Daemon process_path stack buffer overflow attempt (1:15364)	0.00%	28
12585	SERVER-WEBAPP nessus 2.x 404 probe (1:2585)	0.00%	28
314772	WEB-CLIENT libpng malformed chunk denial of service attempt (3:14772)	0.00%	28
125661	MALWARE-CNC Win.Trojan.Buzus variant outbound connection (1:25661)	0.00%	27
116075	SQL Suspicious SQL ansi_padding option (1:16075)	0.00%	27
124169	MALWARE-CNC Win.Trojan.Zbot variant outbound connection (1:24169)	0.00%	26
12228	SERVER-WEBAPP phpMyAdmin db_details_importdocsql.php access (1:2228)	0.00%	26

Rule	Message	%	#
123281	FILE-OFFICE Microsoft Office SharePoint scriptresx.ashx XSS attempt (1:23281)	0.00%	25
125259	MALWARE-CNC Win.Trojan.BancosBanload outbound connection (1:25259)	0.00%	25
118757	INDICATOR-COMPROMISE Microsoft cmd.exe banner Windows Vista (1:18757)	0.00%	24
11844	PROTOCOL-IMAP authenticate overflow attempt (1:1844)	0.00%	24
125552	SERVER-OTHER Rails JSON to YAML parsing deserialization attempt (1:25552)	0.00%	24
125528	SERVER-WEBAPP Moveable Type unauthenticated remote command execution attempt (1:25528)	0.00%	23
113512	SQL generic sql exec injection attempt - GET parameter (1:13512)	0.00%	23
124372	DOS Kerberos KDC null pointer dereference denial of service attempt (1:24372)	0.00%	22

Rule	Message	%	#
114610	SERVER-WEBAPP Joomla invalid token administrative password reset attempt (1:14610)	0.00%	21
121526	BLACKLIST User-Agent known malicious user agent TCYWinHTTPDownload (1:21526)	0.00%	20
115991	DNS Multiple vendor DNS message decompression denial of service attempt (1:15991)	0.00%	20
116271	MALWARE-CNC Trojan.TDSS.1.Gen keepalive detection (1:16271)	0.00%	20
121555	MALWARE-OTHER Horde javascript.php href backdoor (1:21555)	0.00%	20
318211	NETBIOS Microsoft Movie Maker hhctrl.ocx dll-load exploit attempt (3:18211)	0.00%	20
118985	POLICY-OTHER CA ARCserve Axis2 default credential login attempt (1:18985)	0.00%	20
115172	POLICY-SOCIAL XBOX avatar retrieval request (1:15172)	0.00%	20

Rule	Message	%	#
116309	SERVER-ORACLE auth_sesskey buffer overflow attempt (1:16309)	0.00%	19
317428	WEB-MISC Microsoft ASP.NET information disclosure attempt (3:17428)	0.00%	19
11980	MALWARE-BACKDOOR DeepThroat 3.1 Connection (1:1980)	0.00%	18
116495	BOTNET-CNC Rustock botnet contact to C&C server attempt (1:16495)	0.00%	17
115991	DELETED DNS Multiple vendor DNS message decompression denial of service attempt (1:15991)	0.00%	17
117510	FILE-IDENTIFY Microsoft Windows .NET Deploy file download request (1:17510)	0.00%	17
120754	MALWARE-CNC Win.Trojan.Virut-3 outbound connection (1:20754)	0.00%	17
15906	PUA-ADWARE Adware download accelerator plus runtime detection - update (1:5906)	0.00%	17
15803	PUA-TOOLBARS Trackware myway	0.00%	17

Rule	Message	%	#
	speedbar / mywebsearch toolbar runtime detection - collect information (1:5803)		
117340	INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case decoder (1:17340)	0.00%	16
123334	MALWARE-CNC Trojan.Downloader initial C&C checkin (1:23334)	0.00%	16
13456	MYSQL 4.0 root login attempt (1:3456)	0.00%	16
116703	SERVER-MYSQL Database COM_FIELD_LIST Buffer Overflow attempt (1:16703)	0.00%	16
113554	SERVER-OTHER Sybase SQL Anywhere Mobilink version string buffer overflow (1:13554)	0.00%	16
116613	INDICATOR-COMPROMISE c99shell.php command request - cmd (1:16613)	0.00%	15
116624	INDICATOR-COMPROMISE c99shell.php command request - feedback (1:16624)	0.00%	15

Rule	Message	%	#
121538	BOTNET-CNC W32.Dofoil variant outbound payload request (1:21538)	0.00%	14
113583	FILE-IDENTIFY Microsoft SYmbolic LinK file download request (1:13583)	0.00%	14
1495	INDICATOR-COMPROMISE command error (1:495)	0.00%	14
17729	MALWARE-BACKDOOR radmin runtime detection - server-to-client (1:7729)	0.00%	14
113916	SERVER-OTHER Alt-N SecurityGateway username buffer overflow attempt (1:13916)	0.00%	14
14990	SQL heap-based overflow attempt (1:4990)	0.00%	14
315683	WEB-MISC ISA Server OTP-based Forms-authorization fallback policy bypass attempt (3:15683)	0.00%	14
124638	EXPLOIT-KIT Blackholev2 redirection successful (1:24638)	0.00%	13
121682	EXPLOIT-KIT Bleeding Life exploit module call (1:21682)	0.00%	13

Rule	Message	%	#
125052	EXPLOIT-KIT Redkit Exploit Kit Java Exploit requested - 3 digit (1:25052)	0.00%	13
120010	MALWARE-CNC Win32/Babmote.A runtime TCP traffic detected (1:20010)	0.00%	13
113552	SERVER-OTHER Symantec VERITAS Storage Foundation Suite buffer overflow attempt (1:13552)	0.00%	13
313879	WEB-CLIENT Windows BMP image conversion arbitrary code execution attempt (3:13879)	0.00%	13
316167	DOS Microsoft LSASS integer wrap denial of service attempt (3:16167)	0.00%	12
116614	INDICATOR-COMPROMISE c99shell.php command request - search (1:16614)	0.00%	12
116812	MALWARE-CNC known command and control channel traffic (1:16812)	0.00%	12
121528	MALWARE-CNC Trojan.Downloader keep-alive connection detection (1:21528)	0.00%	12

Rule	Message	%	#
119363	MALWARE-CNC Win.Trojan.Dorkbot.B outbound connection (1:19363)	0.00%	12
315365	WEB-CLIENT Microsoft Excel extrst record arbitrary code excecution attempt (3:15365)	0.00%	12
121593	BOTNET-CNC Trojan.Dropper-23836 outbound connection (1:21593)	0.00%	11
121242	MALWARE-CNC Win.Trojan.MsUpdater outbound connection (1:21242)	0.00%	11
116707	MYSQL mysql_log COM_CREATE_DB format string vulnerability exploit attempt (1:16707)	0.00%	11
116606	ORACLE BEA WebLogic Server Plug-ins Certificate overflow attempt (1:16606)	0.00%	11
116551	BLACKLIST User-Agent known malicious user agent - malware (1:16551)	0.00%	10
122088	EXPLOIT-KIT Blackhole Exploit Kit javascript service method (1:22088)	0.00%	10

Rule	Message	%	#
125325	EXPLOIT-KIT Cool Exploit Kit pdf exploit retrieval (1:25325)	0.00%	10
17722	MALWARE-CNC prorat 1.9 cgi notification detection (1:7722)	0.00%	10
121850	MALWARE-CNC TDS Sutra - request hi.cgi (1:21850)	0.00%	10
18497	SQL sp_oacreate vulnerable function attempt (1:8497)	0.00%	10
124792	BLACKLIST User-Agent known malicious user-agent - Google page (1:24792)	0.00%	9
125384	EXPLOIT-KIT Multiple Exploit Kit Payload detection - contacts.exe (1:25384)	0.00%	9
17672	MALWARE-BACKDOOR remoter runtime detection - initial connection (1:7672)	0.00%	9
125577	MALWARE-CNC Win.Rootkit.Necurs possible URI with encrypted POST (1:25577)	0.00%	9
117639	NETBIOS Samba Root File System access bypass attempt (1:17639)	0.00%	9

Rule	Message	%	#
125267	SERVER-OTHER Adobe ColdFusion Admin API arbitrary command execution attempt (1:25267)	0.00%	9
113522	SERVER-OTHER Firebird Database Server username handling buffer overflow (1:13522)	0.00%	9
116674	SERVER-WEBAPP HP OpenView CGI parameter buffer overflow attempt (1:16674)	0.00%	9
124804	SERVER-WEBAPP Invision IP Board PHP unserialize code execution attempt (1:24804)	0.00%	9
118293	SPECIFIC-THREATS Secure Backup login.php uname variable based command injection attempt (1:18293)	0.00%	9
121678	EXPLOIT-KIT Bleeding Life exploit module call (1:21678)	0.00%	8
123219	EXPLOIT-KIT Redkit Java Exploit request to .class file (1:23219)	0.00%	8
113988	INDICATOR-OBFUSCATION large number of calls to ascii function - possible sql	0.00%	8

Rule	Message	%	#
	injection obfuscation (1:13988)		
113987	INDICATOR-OBFUSCATION oversized convert statement - possible sql injection obfuscation (1:13987)	0.00%	8
11981	MALWARE-BACKDOOR DeepThroat 3.1 Connection attempt on port 3150 (1:1981)	0.00%	8
11983	MALWARE-BACKDOOR DeepThroat 3.1 Connection attempt on port 4120 (1:1983)	0.00%	8
1218	MALWARE-BACKDOOR MISC Solaris 2.5 attempt (1:218)	0.00%	8
120008	MALWARE-CNC Malware PDFMarca.A runtime traffic detected (1:20008)	0.00%	8
1463	PROTOCOL-ICMP unassigned type 7 undefined code (1:463)	0.00%	8
123485	SERVER-WEBAPP Wordpress Invit0r plugin php upload attempt (1:23485)	0.00%	8

Rule	Message	%	#
18496	SQL sp_oacreate unicode vulnerable function attempt (1:8496)	0.00%	8
1100002	AgenBola (1:1000002)	0.00%	7
115909	FILE-MULTIMEDIA Apple QuickTime VR Track Header Atom heap corruption attempt (1:15909)	0.00%	7
125807	MALWARE-CNC Win.Trojan.Urausy Botnet variant outbound communication (1:25807)	0.00%	7
113363	SERVER-OTHER Cisco Unified Communications Manager heap overflow attempt (1:13363)	0.00%	7
124435	SERVER-WEBAPP Novell ZENworks Asset Management default admin credentials function call attempt (1:24435)	0.00%	7
123058	SPECIFIC-THREATS NeoSploit Malvertising - URI Requested (1:23058)	0.00%	7
313626	WEB-CLIENT Microsoft Access download attempt (3:13626)	0.00%	7
12091	WEB-IIS WEBDAV nessus safe scan attempt (1:2091)	0.00%	7

Rule	Message	%	#
116008	WEB-MISC Multiple Products excessive HTTP 304 Not Modified responses exploit attempt (1:16008)	0.00%	7
112633	DELETED EXPLOIT Microsoft Windows 2000 Kodak Imaging small offset malformed tiff (1:12633)	0.00%	6
118330	DELETED NETBIOS Adobe multiple products dwmapi.dll dll-load exploit attempt (1:18330)	0.00%	6
117483	DNS squid proxy dns A record response denial of service attempt (1:17483)	0.00%	6
125383	EXPLOIT-KIT Multiple Exploit Kit Payload detection - info.exe (1:25383)	0.00%	6
121786	INDICATOR-OBFUSCATION encoded javascript escape function in POST parameters - likely javascript injection (1:21786)	0.00%	6
117337	INDICATOR-SHELLCODE x86 Microsoft Win32 export tabel enumeration variant (1:17337)	0.00%	6

Rule	Message	%	#
116144	MALWARE-CNC Bredolab bot variant outbound connection (1:16144)	0.00%	6
123631	SERVER-APACHE Apache Struts remote code execution attempt - POST parameter (1:23631)	0.00%	6
12063	SERVER-WEBAPP Demarc SQL injection attempt (1:2063)	0.00%	6
118431	WEB-CLIENT Acrobat Reader plugin sqlite.dll dll-load exploit attempt (1:18431)	0.00%	6
316222	WEB-CLIENT Malformed BMP dimensions arbitrary code execution attempt (3:16222)	0.00%	6
318210	WEB-CLIENT Microsoft Movie Maker hhctrl.ocx dll-load exploit attempt (3:18210)	0.00%	6
11002	WEB-IIS cmd.exe access (1:1002)	0.00%	6
123473	BLACKLIST URI request for runforestrun - JS.Runfore (1:23473)	0.00%	5
121488	BLACKLIST USER-AGENT known malicious user agent GetRight (1:21488)	0.00%	5

Rule	Message	%	#
121681	EXPLOIT-KIT Bleeding Life exploit module call (1:21681)	0.00%	5
125593	EXPLOIT-KIT Cool Exploit Kit java exploit retrieval (1:25593)	0.00%	5
125507	EXPLOIT-KIT Cool Exploit Kit pdf exploit retrieval (1:25507)	0.00%	5
125386	EXPLOIT-KIT Multiple Exploit Kit Payload detection - about.exe (1:25386)	0.00%	5
118549	FILE-OFFICE Microsoft Office Word with embedded Flash file attachment (1:18549)	0.00%	5
116623	INDICATOR-COMPROMISE c99shell.php command request - eval (1:16623)	0.00%	5
121783	INDICATOR-OBFUSCATION encoded script tag in POST parameters - likely cross-site scripting (1:21783)	0.00%	5
1152	MALWARE-BACKDOOR BackConstruction 2.1 Connection (1:152)	0.00%	5
122034	MALWARE-CNC Apple OSX Flashback malware	0.00%	5

Rule	Message	%	#
	outbound connection (1:22034)		
120683	MALWARE-CNC Cleanvaccine variant outbound connection (1:20683)	0.00%	5
125660	MALWARE-CNC Win.Trojan.Medfos variant outbound connection (1:25660)	0.00%	5
119157	POLICY-OTHER HP Universal CMDB server axis2 default credentials attempt (1:19157)	0.00%	5
117331	SERVER-MAIL IBM Lotus Notes HTML Speed Reader Long URL buffer overflow attempt (1:17331)	0.00%	5
18715	SERVER-WEBAPP cacti graph_image SQL injection attempt (1:8715)	0.00%	5
118613	SERVER-WEBAPP Oracle Java Web Server WebDAV Stack Buffer Overflow attempt (1:18613)	0.00%	5
112009	SQL Firebird SQL Fbserver buffer overflow attempt (1:12009)	0.00%	5
112286	WEB-CLIENT PCRE character class double free	0.00%	5

Rule	Message	%	#
	overflow attempt (1:12286)		
315327	BAD-TRAFFIC libspf2 DNS TXT record parsing buffer overflow attempt (3:15327)	0.00%	4
315386	BAD-TRAFFIC wpad dynamic update request (3:15386)	0.00%	4
122058	BOTNET-CNC Trojan.Kbot variant outbound connection (1:22058)	0.00%	4
118328	DELETED WEB-CLIENT Adobe multiple products dwmapi.dll dll-load exploit attempt (1:18328)	0.00%	4
125387	EXPLOIT-KIT Multiple Exploit Kit Payload detection - readme.exe (1:25387)	0.00%	4
121941	INDICATOR-COMPROMISE Wordpress Request for php file in fgallery directory (1:21941)	0.00%	4
111317	MALWARE-BACKDOOR abremote pro 3.1 runtime detection - init connection (1:11317)	0.00%	4

Rule	Message	%	#
1210	MALWARE-BACKDOOR attempt (1:210)	0.00%	4
123051	MALWARE-CNC Dybalom.A runtime traffic detected (1:23051)	0.00%	4
121239	MALWARE-CNC W32.Kazy variant outbound connection (1:21239)	0.00%	4
120233	MALWARE-CNC Win.Trojan.Virut outbound connection (1:20233)	0.00%	4
19326	MALWARE-OTHER netsky.p smtp propagation detection (1:9326)	0.00%	4
19378	MALWARE-OTHER netsky.q smtp propagation detection (1:9378)	0.00%	4
318435	NETBIOS Acrobat Reader IE plugin agm.dll dll-load exploit attempt (3:18435)	0.00%	4
116935	POLICY-SPAM sjtu-edp.cn known spam email attempt (1:16935)	0.00%	4
13670	SERVER-MYSQL secure client overflow attempt (1:3670)	0.00%	4
110187	SERVER-OTHER HP Mercury Loadrunner	0.00%	4

Rule	Message	%	#
	command line buffer overflow (1:10187)		
118795	SERVER-WEBAPP HP OpenView Network Node Manager ovet_demandpoll.exe format string execution attempt (1:18795)	0.00%	4
124642	SERVER-WEBAPP RedHat JBoss Enterprise Application Platform JMX code execution attempt (1:24642)	0.00%	4
123783	SERVER-WEBAPP Symantec Web Gateway pbcontrol.php filename parameter command injection attempt (1:23783)	0.00%	4
318441	WEB-CLIENT Acrobat Reader IE plugin bibutils.dll dll-load exploit attempt (3:18441)	0.00%	4
313824	WEB-CLIENT malformed mjpeg arbitrary code execution attempt (3:13824)	0.00%	4
315117	WEB-CLIENT Microsoft Excel malformed OBJ record arbitrary code execution attempt (3:15117)	0.00%	4

Rule	Message	%	#
316156	WEB-CLIENT Windows Media Player ASF marker object memory corruption attempt (3:16156)	0.00%	4
11385	WEB-MISC mod-plsql administration access (1:1385)	0.00%	4
317731	BAD-TRAFFIC wpad dynamic update request (3:17731)	0.00%	3
116812	BOTNET-CNC known command and control channel traffic (1:16812)	0.00%	3
121547	BOTNET-CNC Win32.Trojan.Kazy variant outbound connection attempt (1:21547)	0.00%	3
318425	DELETED NETBIOS Firefox Acrobat Reader cooltype.dll dll-load exploit attempt - DISABLED (3:18425)	0.00%	3
318428	DELETED WEB-CLIENT Firefox Acrobat Reader agm.dll dll-load exploit attempt - DISABLED (3:18428)	0.00%	3
125385	EXPLOIT-KIT Multiple Exploit Kit Payload detection - calc.exe (1:25385)	0.00%	3

Rule	Message	%	#
116617	INDICATOR-COMPROMISE c99shell.php command request - encoder (1:16617)	0.00%	3
19834	MALWARE-BACKDOOR ieva 1.0 runtime detection - black screen (1:9834)	0.00%	3
120064	MALWARE-CNC Malware Win.Trojan.Clemag.A variant outbound connection (1:20064)	0.00%	3
122937	MALWARE-CNC Trojan.Proxyier outbound connection (1:22937)	0.00%	3
112661	MALWARE-CNC troll.a outbound connection (1:12661)	0.00%	3
125257	MALWARE-CNC Win.Trojan.Skintrim outbound connection (1:25257)	0.00%	3
113593	MYSQL yaSSL SSL Hello Message Buffer Overflow attempt (1:13593)	0.00%	3
113712	MYSQL yaSSL SSLv2 Client Hello Message Session ID Buffer Overflow attempt (1:13712)	0.00%	3

Rule	Message	%	#
318209	NETBIOS Windows 7 Home peerdist.dll dll-load exploit attempt (3:18209)	0.00%	3
121934	PUA-ADWARE 888Poker install outbound connection attempt (1:21934)	0.00%	3
124697	SERVER-APACHE Apache mod_log_config cookie handling denial of service attempt (1:24697)	0.00%	3
125370	SERVER-OTHER CakePHP unserialize method vulnerability exploitation attempt (1:25370)	0.00%	3
121235	SERVER-WEBAPP LOCK Webdav Stack Buffer Overflow attempt (1:21235)	0.00%	3
111193	SERVER-WEBAPP Oracle iSQL Plus cross site scripting attempt (1:11193)	0.00%	3
121686	SPECIFIC-THREATS Bleeding Life exploit module call (1:21686)	0.00%	3
19331	SPECIFIC-THREATS mydoom.m smtp propagation detection (1:9331)	0.00%	3

Rule	Message	%	#
316183	WEB-CLIENT Microsoft .NET MSIL CombineImpl suspicious usage (3:16183)	0.00%	3
318277	WEB-CLIENT Vista Backup Tool fveapi.dll dll-load exploit attempt (3:18277)	0.00%	3
116303	BOTNET-CNC Virut DNS request attempt (1:16303)	0.00%	2
314263	CHAT Pidgin MSN MSNP2P message integer overflow attempt (3:14263)	0.00%	2
318423	DELETED NETBIOS Firefox Acrobat Reader agm.dll dll-load exploit attempt - DISABLED (3:18423)	0.00%	2
13821	DELETED WEB-CLIENT CHM file transfer attempt (1:3821)	0.00%	2
113519	EXPLOIT Citrix MetaFrame IMA buffer overflow attempt (1:13519)	0.00%	2
121071	EXPLOIT-KIT Eleanore exploit kit post-exploit page request (1:21071)	0.00%	2
123705	FILE-IDENTIFY Ultimate Packer for Executabels/UPX v0.62-	0.00%	2

Rule	Message	%	#
	v1.22 packed file magic detected (1:23705)		
116560	FILE-OFFICE Microsoft Office SharePoint XSS attempt (1:16560)	0.00%	2
118526	FILE-PDF Adobe Reader shell metacharacter code execution attempt (1:18526)	0.00%	2
117338	INDICATOR-SHELLCODE x86 Microsoft Windows 32-bit SEH get EIP technique (1:17338)	0.00%	2
116487	MALWARE-BACKDOOR Arucer backdoor traffic - yes command attempt (1:16487)	0.00%	2
1141	MALWARE-BACKDOOR HackAttack 1.20 Connect (1:141)	0.00%	2
19836	MALWARE-BACKDOOR ieva 1.0 runtime detection - crazy mouse (1:9836)	0.00%	2
17822	MALWARE-BACKDOOR xbkdr runtime detection (1:7822)	0.00%	2
17103	MALWARE-CNC gwboy 0.92 variant outbound connection (1:7103)	0.00%	2

Rule	Message	%	#
1989	MALWARE-CNC sensepost.exe command shell (1:989)	0.00%	2
120661	MALWARE-CNC Simbda variant outbound connection (1:20661)	0.00%	2
125570	MALWARE-CNC WIN.Trojan.Medialabs outbound connection (1:25570)	0.00%	2
311619	MISC MySQL COM_TABEL_DUMP Function Stack Overflow attempt (3:11619)	0.00%	2
314253	MULTIMEDIA Windows Media Player malicious playlist buffer overflow attempt (3:14253)	0.00%	2
314254	MULTIMEDIA Windows Media Player malicious playlist buffer overflow attempt (3:14254)	0.00%	2
113711	MYSQL yaSSL SSLv2 Client Hello Message Cipher Length Buffer Overflow attempt (1:13711)	0.00%	2
318426	NETBIOS Firefox Acrobat Reader sqlite.dll dll-load exploit attempt (3:18426)	0.00%	2
13032	NETBIOS SMB-DS NT Trans NT CREATE	0.00%	2

Rule	Message	%	#
	unicode SACL overflow attempt (1:3032)		
318278	NETBIOS Vista Backup Tool fveapi.dll dll-load exploit attempt (3:18278)	0.00%	2
118211	OS-WINDOWS Microsoft Movie Maker hhctrl.ocx dll-load exploit attempt (1:18211)	0.00%	2
117012	POLICY-SPAM oneus.ru known spam email attempt (1:17012)	0.00%	2
12330	PROTOCOL-IMAP auth overflow attempt (1:2330)	0.00%	2
113555	SERVER-OTHER Sybase SQL Anywhere Mobilink remoteID string buffer overflow (1:13555)	0.00%	2
121234	SERVER-WEBAPP MKCOL Webdav Stack Buffer Overflow attempt (1:21234)	0.00%	2
118905	SERVER-WEBAPP OpenView Network Node Manager cookie buffer overflow attempt (1:18905)	0.00%	2
124256	SERVER-WEBAPP phpMyAdmin server_sync.php backdoor access attempt (1:24256)	0.00%	2

Rule	Message	%	#
121492	SPECIFIC-THREATS Blackhole landing page with specific structure - prototype catch (1:21492)	0.00%	2
15906	SPYWARE-PUT Adware download accelerator plus runtime detection - update (1:5906)	0.00%	2
111264	SQL Microsoft SQL Server 2000 Server hello buffer overflow attempt (1:11264)	0.00%	2
318442	WEB-CLIENT Acrobat Reader IE plugin cooltype.dll dll-load exploit attempt (3:18442)	0.00%	2
115185	APP-DETECT Nintendo Wii SSL Server Hello (1:15185)	0.00%	1
115165	BACKDOOR Pushdo client communication attempt (1:15165)	0.00%	1
125735	BLACKLIST DNS request for known malware domain celebrity-info.com (1:25735)	0.00%	1
123156	BLACKLIST URI Nuclear Pack exploit kit landing page (1:23156)	0.00%	1
121636	BLACKLIST User-Agent known Adware user agent gbot (1:21636)	0.00%	1

Rule	Message	%	#
124633	BLACKLIST User-Agent known malicious user agent - test_hInternet (1:24633)	0.00%	1
121910	BOTNET-CNC Apple OSX Flashback malware user-agent (1:21910)	0.00%	1
118939	BOTNET-CNC known command and control channel traffic (1:18939)	0.00%	1
120754	BOTNET-CNC Win32.Virut-3 outbound connection (1:20754)	0.00%	1
117378	BROWSER-FIREFOX Mozilla Firefox Animated PNG Processing integer overflow attempt (1:17378)	0.00%	1
115497	DELETED FILE-PDF Suspicious JBIG2 pdf file sent with email (1:15497)	0.00%	1
318429	DELETED WEB-CLIENT Firefox Acrobat Reader bibutils.dll dll-load exploit attempt - DISABLED (3:18429)	0.00%	1
115896	DOS Firebird SQL op_connect_request denial of service attempt (1:15896)	0.00%	1
113902	EXPLOIT IBM Lotus Sametime multiplexer	0.00%	1

Rule	Message	%	#
	stack buffer overflow attempt (1:13902)		
124501	EXPLOIT-KIT Blackhole v2 fallback executabel download (1:24501)	0.00%	1
125388	EXPLOIT-KIT Blackholev2 redirection successful (1:25388)	0.00%	1
121680	EXPLOIT-KIT Bleeding Life exploit module call (1:21680)	0.00%	1
121684	EXPLOIT-KIT Bleeding Life exploit module call (1:21684)	0.00%	1
121685	EXPLOIT-KIT Bleeding Life exploit module call (1:21685)	0.00%	1
121099	EXPLOIT-KIT Crimepack exploit kit malicious pdf request (1:21099)	0.00%	1
121043	EXPLOIT-KIT URI possible Blackhole post-compromise download attempt - .php?e= (1:21043)	0.00%	1
121041	EXPLOIT-KIT URI possible Blackhole URL - main.php?page= (1:21041)	0.00%	1
120558	EXPLOIT-KIT URI request for known	0.00%	1

Rule	Message	%	#
	malicious URI /stat2.php (1:20558)		
124975	FILE-OFFICE Microsoft Office Word rtf invalid listoverridecount value attempt (1:24975)	0.00%	1
115358	FILE-PDF Adobe Reader JBIG2 remote code execution attempt (1:15358)	0.00%	1
125819	FILE-PDF Adobe Reader known malicious variable (1:25819)	0.00%	1
123830	INDICATOR-COMPROMISE Alsa3ek Web Shell (1:23830)	0.00%	1
116620	INDICATOR-COMPROMISE c99shell.php command request - ftpquickbrute (1:16620)	0.00%	1
120184	INDICATOR-SHELLCODE Metasploit php meterpreter stub .php file upload (1:20184)	0.00%	1
117324	INDICATOR-SHELLCODE x86 Linux reverse connect shellcode (1:17324)	0.00%	1
117345	INDICATOR-SHELLCODE x86 OS agnostic dword additive	0.00%	1

Rule	Message	%	#
	feedback decoder (1:17345)		
17636	MALWARE-BACKDOOR hornet 1.0 runtime detection - fetch processes list (1:7636)	0.00%	1
19835	MALWARE-BACKDOOR ieva 1.0 runtime detection - swap mouse (1:9835)	0.00%	1
16027	MALWARE-BACKDOOR netshadow runtime detection (1:6027)	0.00%	1
123341	MALWARE-BACKDOOR Win.Backdoor.Tinrot.A runtime detection (1:23341)	0.00%	1
110196	MALWARE-BACKDOOR Wordpress backdoor feed.php code execution (1:10196)	0.00%	1
121047	MALWARE-CNC known malicious SSL certificate - Sykipot C&C (1:21047)	0.00%	1
116440	MALWARE-CNC Possible Zeus User-Agent - ie (1:16440)	0.00%	1
120877	MALWARE-CNC RunTime Worm.Win32.Warezov.gs	0.00%	1

Rule	Message	%	#
	outbound connection (1:20877)		
119569	MALWARE-CNC Trojan-Downloader.Win32.Perkesh outbound connection (1:19569)	0.00%	1
121518	MALWARE-CNC Trojan.Agent-59544 connect to server (1:21518)	0.00%	1
121523	MALWARE-CNC Trojan.Kazy variant outbound connection (1:21523)	0.00%	1
122056	MALWARE-CNC Trojan.Kazy variant outbound connection (1:22056)	0.00%	1
121959	MALWARE-CNC UPDATE communication protocol connection to server (1:21959)	0.00%	1
118936	MALWARE-CNC URI request for known malicious URI - Win.Trojan.FakeAV (1:18936)	0.00%	1
118945	MALWARE-CNC Virus.Win32.Feberr variant outbound connection (1:18945)	0.00%	1
119730	MALWARE-CNC Win.Trojan.KukuBot.A	0.00%	1

Rule	Message	%	#
	outbound connection (1:19730)		
125571	MALWARE-CNC WIN.Trojan.Medialabs outbound connection (1:25571)	0.00%	1
19426	MALWARE-OTHER mydoom.ap attachment (1:9426)	0.00%	1
124102	MALWARE-OTHER Possible Kuluoz spamvertised URL in email (1:24102)	0.00%	1
124017	MALWARE-OTHER Possible malicious redirect - rebots.php (1:24017)	0.00%	1
116708	MYSQL mysql_log COM_DROP_DB format string vulnerability exploit attempt (1:16708)	0.00%	1
13667	MYSQL protocol 41 client authentication bypass attempt (1:3667)	0.00%	1
11776	MYSQL show databases attempt (1:1776)	0.00%	1
318437	NETBIOS Acrobat Reader IE plugin cooltype.dll dll-load exploit attempt (3:18437)	0.00%	1

Rule	Message	%	#
118076	OS-WINDOWS Microsoft Forefront UAG URL XSS alternate attempt (1:18076)	0.00%	1
116417	OS-WINDOWS SMB Negotiate Protocol Response overflow attempt (1:16417)	0.00%	1
115171	POLICY-SOCIAL XBOX Marketplace http request (1:15171)	0.00%	1
116524	PROTOCOL-FTP ProFTPD username sql injection attempt (1:16524)	0.00%	1
13068	PROTOCOL-IMAP examine overflow attempt (1:3068)	0.00%	1
121645	PUA-ADWARE Adware.MediaGetInstaller outbound connection - source ip infected (1:21645)	0.00%	1
117156	SERVER-APACHE HP Performance Manager Apache Tomcat policy bypass attempt (1:17156)	0.00%	1
19841	SERVER-MAIL Micrsoft Office Outlook VEVENT overflow attempt (1:9841)	0.00%	1
13669	SERVER-MYSQL protocol 41 secure client overflow attempt (1:3669)	0.00%	1

Rule	Message	%	#
116215	SERVER-ORACLE Oracle Application Server Portal cross site scripting attempt (1:16215)	0.00%	1
116192	SERVER-ORACLE Secure Backup Administration server authentication bypass attempt (1:16192)	0.00%	1
118753	SERVER-OTHER Zend Server Java Bridge remote code execution attempt (1:18753)	0.00%	1
120179	SERVER-WEBAPP HP OpenView NNM ovlogin.exe CGI userid parameter buffer overflow attempt (1:20179)	0.00%	1
124913	SERVER-WEBAPP HP OpenView NNM ovutil.dll getProxiedStorageAddress buffer overflow attempt (1:24913)	0.00%	1
124518	SERVER-WEBAPP Symantec Web Gateway PHP remote code injection attempt (1:24518)	0.00%	1
117597	SERVER-WEBAPP TikiWiki jhot.php script file upload attempt (1:17597)	0.00%	1

Rule	Message	%	#
121236	SERVER-WEBAPP UNLOCK Webdav Stack Buffer Overflow attempt (1:21236)	0.00%	1
121681	SPECIFIC-THREATS Bleeding Life exploit module call (1:21681)	0.00%	1
121860	SPECIFIC-THREATS Phoenix exploit kit post-compromise behavior (1:21860)	0.00%	1
14989	SQL heap-based overflow attempt (1:4989)	0.00%	1
11059	SQL xp_filelist attempt (1:1059)	0.00%	1
11069	SQL xp_regread attempt (1:1069)	0.00%	1
113996	SQL xp_servicecontrol attempt (1:13996)	0.00%	1
113998	SQL xp_terminate_process attempt (1:13998)	0.00%	1
118464	WEB-CGI Adobe ColdFusion locale directory traversal attempt (1:18464)	0.00%	1
1861	WEB-CGI w3-msql access (1:861)	0.00%	1
318443	WEB-CLIENT Acrobat Reader IE plugin cryptocme2.dll dll-load exploit attempt (3:18443)	0.00%	1

Rule	Message	%	#
315517	WEB-CLIENT AVI DirectShow quicktime parsing overflow attempt (3:15517)	0.00%	1
315503	WEB-CLIENT Download of PowerPoint 95 file (3:15503)	0.00%	1
313963	WEB-CLIENT Internet Explorer argument validation in print preview handling vulnerability (3:13963)	0.00%	1
315521	WEB-CLIENT Microsoft Office Excel ExternSheet record remote code execution attempt (3:15521)	0.00%	1
315857	WEB-CLIENT Microsoft Windows AVIFile media file invalid header length (3:15857)	0.00%	1
116522	WEB-CLIENT Novell QuickFinder server cross-site-scripting attempt (1:16522)	0.00%	1
315976	WEB-CLIENT OpenOffice TIFF file in big endian format parsing integer overflow attempt (3:15976)	0.00%	1
315975	WEB-CLIENT OpenOffice TIFF file in	0.00%	1

Rule	Message	%	#
	little endian format parsing integer overflow attempt (3:15975)		
317700	WEB-CLIENT RealNetworks RealPlayer wav chunk string overflow attempt (3:17700)	0.00%	1
116356	WEB-IIS multiple extension code execution attempt (1:16356)	0.00%	1
117609	WEB-MISC Oracle Java Web Server Webdav Stack Buffer Overflow attempt (1:17609)	0.00%	1
118612	WEB-MISC Oracle Java Web Server Webdav Stack Buffer Overflow attempt (1:18612)	0.00%	1
18713	WEB-PHP cacti graph_image SQL injection attempt (1:8713)	0.00%	1
			41,882,878

LAMPIRAN B – NEGARA TUJUAN SERANGAN

Tabel dibawah merupakan negara tujuan beserta jumlah serangan dan jumlah serangan yang dialami.

CountryName	Count
Indonesia	18,780,842
United States	8,579,014
China	1,612,341
Japan	1,328,457
India	1,004,882
Canada	918,522
Taiwan	769,083
Germany	542,668
Romania	498,634
Thailand	463,000
Russia	417,791
Brazil	355,576
France	351,310
Italy	339,985
United Kingdom	333,675
Sweden	326,917
Australia	275,249
Republic of Korea	248,924
Singapore	239,149
Hong Kong	224,516
Argentina	222,696

CountryName	Count
Bulgaria	214,616
Spain	214,167
Philippines	213,301
Netherlands	206,811
Poland	202,004
Venezuela	196,042
Ukraine	192,942
Malaysia	167,875
Vietnam	164,360
Turkey	131,113
Hungary	124,566
Israel	116,003
Colombia	114,534
Chile	97,814
Serbia	92,039
Portugal	89,010
Mexico	87,922
Sudan	78,954
Belgium	75,074
Iran	60,569
Denmark	57,687
Republic of Lithuania	55,925
Belarus	53,423
Bosnia and Herzegovina	52,790
Czech Republic	49,241
Kazakhstan	45,657

CountryName	Count
Pakistan	43,888
Switzerland	43,129
Saudi Arabia	41,697
Monaco	38,435
Norway	36,843
Georgia	36,777
New Zealand	35,981
Latvia	35,538
United Arab Emirates	29,386
Macedonia	27,467
Slovenia	26,277
South Africa	25,544
Croatia	24,132
Republic of Moldova	22,707
Morocco	21,309
Austria	19,886
Finland	18,980
Slovak Republic	16,728
Ireland	16,128
Greece	15,588
Panama	14,611
Bangladesh	13,546
Algeria	13,358
Uruguay	13,135
Armenia	13,073
Costa Rica	12,788

CountryName	Count
Trinidad and Tobago	11,565
Mongolia	11,535
Iraq	11,527
Estonia	11,372
Ecuador	8,537
Puerto Rico	8,223
Bahamas	6,962
Albania	6,399
Egypt	6,205
Tunisia	6,110
Montenegro	6,008
Nigeria	5,972
Qatar	5,827
Peru	5,662
Kyrgyzstan	5,539
Macao	5,050
Paraguay	4,966
Cyprus	4,764
Belize	4,414
Azerbaijan	4,355
Sri Lanka	4,165
Jamaica	3,864
Cambodia	3,666
Malta	3,420
Angola	3,397
Hashemite Kingdom of Jordan	3,144

CountryName	Count
Bolivia	3,045
Brunei	3,043
Kuwait	2,809
Luxembourg	2,797
Guatemala	2,768
Palestine	2,318
Kenya	2,091
Isle of Man	2,073
El Salvador	1,959
Nepal	1,920
Myanmar [Burma]	1,909
Tanzania	1,843
Saint Kitts and Nevis	1,834
Laos	1,775
Guam	1,758
Dominican Republic	1,624
Oman	1,618
Mozambique	1,513
Honduras	1,497
New Caledonia	1,452
Nicaragua	1,382
Fiji	1,366
Saint Vincent and the Grenadines	1,352
Uzbekistan	1,344
Guyana	1,326
Mauritius	1,130

CountryName	Count
British Virgin Islands	1,127
Afghanistan	1,089
Lebanon	1,065
Maldives	1,020
Bahrain	1,000
Ivory Coast	909
CuraÃ§ao	900
Iceland	885
Syria	862
Ghana	852
Namibia	725
Grenada	708
Madagascar	674
Northern Mariana Islands	630
Turkmenistan	613
Senegal	608
Saint Lucia	582
Cameroon	554
Zambia	541
Bermuda	532
Kosovo	529
Zimbabwe	453
Tajikistan	439
Andorra	426
Seychelles	416
Guernsey	372

CountryName	Count
Barbados	361
San Marino	346
Yemen	344
Cayman Islands	325
Papua New Guinea	302
Liechtenstein	277
Bhutan	275
Aruba	265
RÃ©union	265
Uganda	263
Gabon	251
French Polynesia	250
Guadeloupe	221
Malawi	218
Rwanda	200
Botswana	200
Martinique	199
Dominica	196
East Timor	187
Suriname	167
Mali	162
Libya	154
Federated States of Micronesia	144
Sint Maarten	135
French Guiana	125
Congo	116

CountryName	Count
Djibouti	108
U.S. Virgin Islands	103
American Samoa	99
Haiti	89
Ethiopia	77
Bonaire	
Gibraltar	67
Marshall Islands	65
Antigua and Barbuda	65
Cuba	64
Jersey	62
Tonga	62
Lesotho	61
Niger	59
Mauritania	55
Saint Martin	54
Guinea	42
Turks and Caicos Islands	35
Burkina Faso	33
Gambia	27
Togo	27
Benin	24
Anguilla	20
Chad	19
Liberia	18
Cape Verde	18

CountryName	Count
SÃ£o TomÃ© and PrÃncipe	18
Equatorial Guinea	17
Republic of the Congo	14
Falkland Islands	13
Mayotte	13
Eritrea	11
Vatican City	11
Palau	11
Solomon Islands	10
Faroe Islands	10
Sierra Leone	10
Vanuatu	9
Swaziland	7
North Korea	6
Comoros	5
Montserrat	5
Greenland	5
Kiribati	4
Wallis and Futuna	4
Saint Pierre and Miquelon	3
Saint-BarthÃ©lemy	3
South Sudan	3
Samoa	2
Ã…land	2
Tuvalu	2
Burundi	1

CountryName	Count
British Indian Ocean Territory	1

LAMPIRAN C – NEGARA PENYERANG

Tabel dibawah merupakan negara penyerang beserta jumlah serangan yang dilakukan

CountryName	Count
Indonesia	27,759,147
China	7,627,189
Argentina	1,805,874
United States	1,090,489
France	700,930
Brazil	403,888
Russia	324,434
Netherlands	240,119
Taiwan	229,343
India	165,218
Canada	133,553
Germany	104,081
Vietnam	101,432
Hong Kong	88,699
Thailand	82,189
Japan	79,218
Mexico	73,883
Singapore	69,055
Ukraine	58,389
Republic of Korea	54,602
Philippines	54,509
Republic of Lithuania	49,653
Malaysia	43,961

CountryName	Count
Australia	41,967
United Kingdom	37,135
Israel	33,676
Turkey	32,432
Spain	30,334
Egypt	25,990
Italy	25,294
Estonia	24,122
Algeria	24,106
Chile	19,718
Romania	16,673
Bulgaria	15,876
Poland	13,464
Venezuela	13,306
Pakistan	12,021
Latvia	10,694
Sweden	10,640
Saudi Arabia	9,673
Ireland	8,476
Belgium	8,319
null	7,813
Morocco	6,851
New Zealand	5,723
United Arab Emirates	5,360
Switzerland	4,932
Hashemite Kingdom of Jordan	4,742

CountryName	Count
Iran	4,563
Denmark	4,232
Colombia	3,923
South Africa	3,531
Bahrain	3,287
Portugal	3,147
Ecuador	3,140
Dominican Republic	2,963
Albania	2,917
Serbia	2,718
Hungary	2,498
Greece	2,471
Bangladesh	2,269
Sri Lanka	2,202
Republic of Moldova	1,990
Peru	1,889
Cambodia	1,862
Austria	1,762
Paraguay	1,724
Kazakhstan	1,620
Czech Republic	1,605
Bosnia and Herzegovina	1,600
Norway	1,574
Tunisia	1,540
Palestine	1,475
Tanzania	1,392

CountryName	Count
Belarus	1,372
Belize	1,351
Guam	1,345
Luxembourg	1,333
Nigeria	1,128
Finland	1,094
Nepal	1,085
Slovak Republic	967
Qatar	861
Iraq	781
Maldives	766
Bolivia	748
Armenia	730
Kuwait	727
Uruguay	688
Macedonia	677
Slovenia	674
Lebanon	670
Azerbaijan	635
Syria	623
Croatia	532
Myanmar [Burma]	521
Senegal	509
Georgia	460
Kenya	388
Laos	386

CountryName	Count
Macao	382
El Salvador	341
Trinidad and Tobago	341
Barbados	340
Costa Rica	333
Iceland	332
Mauritius	329
Libya	324
Cyprus	318
Yemen	302
Guatemala	277
Panama	264
Mongolia	258
Malta	244
Sudan	241
Brunei	238
Cameroon	230
Afghanistan	194
Mali	178
Puerto Rico	177
Ivory Coast	155
Honduras	148
Kyrgyzstan	141
Oman	140
Bahamas	140
Uzbekistan	138

CountryName	Count
Montenegro	129
Ghana	128
Ethiopia	113
Gabon	98
Jamaica	97
Benin	91
Suriname	90
Mozambique	85
Bonaire, Sint Eustatius, and Saba	71
New Caledonia	69
East Timor	66
Djibouti	66
Bhutan	59
Uganda	53
Angola	49
Tajikistan	45
Mauritania	42
Zimbabwe	42
Papua New Guinea	40
Nicaragua	40
Madagascar	38
Namibia	37
Fiji	36
Seychelles	34
Monaco	30
Bermuda	30

CountryName	Count
Haiti	28
R,union	27
Guadeloupe	25
Grenada	22
Cura‡ao	21
Togo	20
Botswana	18
Martinique	18
Malawi	18
Cayman Islands	17
Zambia	16
Burkina Faso	15
Isle of Man	14
Aruba	14
Jersey	14
Congo	13
Northern Mariana Islands	13
Greenland	13
Tonga	13
Saint Vincent and the Grenadines	12
French Guiana	12
French Polynesia	11
San Marino	11
Niger	10
Sierra Leone	10
Guyana	9

CountryName	Count
British Virgin Islands	9
Saint Lucia	8
Rwanda	7
Gambia	7
Faroe Islands	7
Cape Verde	7
Antigua and Barbuda	7
Turks and Caicos Islands	6
American Samoa	6
Turkmenistan	6
South Sudan	6
Federated States of Micronesia	6
Lesotho	6
Liechtenstein	5
Sint Maarten	5
Gibraltar	5
Somalia	4
U.S. Virgin Islands	4
Saint Kitts and Nevis	4
Marshall Islands	3
Andorra	3
Guernsey	3
Saint Pierre and Miquelon	3
Burundi	2
Solomon Islands	2
Eritrea	2

CountryName	Count
Dominica	2
Republic of the Congo	2
Saint Martin	1
Liberia	1
Mayotte	1
Saint-Barth,lemy	1
Anguilla	1
Palau	1
Swaziland	1
S?o Tom, and Pr¡ncipe	1

BAB VII
KESIMPULAN

Bab ini merupakan kesimpulan dari hasil penelitian ini dan juga memberikan saran untuk perbaikan penelitian selanjutnya. Selain itu juga dapat digunakan sebagai

7.1 Kesimpulan

Dari hasil pengolahan data pada penelitian ini, ditemukan bahwa serangan yang terjadi di Indonesia cukup banyak jenisnya, yaitu sebanyak 620 jenis dari 41 juta serangan yang tercatat pada bulan Januari hingga Oktober. Namun dari sekian banyak serangan tersebut, lebih dari 90% didominasi oleh 8 jenis serangan saja. Selain hal tersebut, 34 juta serangan tersebut merupakan serangan yang memiliki prioritas tinggi sehingga dapat dikatakan berbahaya.

Berdasarkan data bulanan, bulan Maret merupakan bulan dengan erangan tertinggi. Tercatat pada tanggal 19 Maret 2013 memiliki jumlah serangan tertinggi sebanyak 442516. Sedangkan bulan Februari tercatat memiliki jumlah serangan terendah.

Selain itu, berdasarkan lokasi, Indonesia merupakan negara penyerang dengan serangan terbanyak sebanyak 25 juta serangan dan juga sebagai negara yang paling banyak diserang dengan sebanyak 18 juta serangan. Hal ini wajar mengingat lokasi sensor berada di Indonesia.

Secara karakteristik, Malware Zero Access memiliki jumlah terbanyak (sebanyak 37% dari total serangan), hal itu terjadi sebab pada tahun 2013 Malware Zero Access menyebar luas diberbagai negara. Walaupun jumlah serangannya cukup besar, serangan jenis ini tidak termasuk pada serangan-seranganyang *frequent* dibandingkan jenis serangan yang lain.

Pada SQL Attack, serangan yang sering terjadi adalah ***brute force login, client authentication bypass dan login attempt from unauthorized version.*** Serangan tersebut merupakan serangan yang mengancam pada kredensial dari SQL itu

sendiri, sehingga apabila serangan tersebut terjadi maka kemungkinan penyerang akan dapat mengakses SQL secara remote. Sedangkan serangan seperti ***SQL Union attack, version overflow*** terjadi untuk mengambil data yang penting dari segi aplikasi. Serangan ini umum disebut ***blind sql injection*** dimana penyerang mencoba mengambil celah dengan menggunakan illegal character pada SQL. Lalu terjadi SQL Worm propagation attempt yang dapat mengakibatkan DoS MSDTC Attempt, yaitu worm yang menargetkan pada MSDTC client, yaitu SQL Server 2008 dan Windows Server.

Terdapat juga serangan yang irrelevan, yaitu Malware CNC, yang merupakan Malware TDS Sutra. Malware ini menargetkan serangan ke DNS sehingga kemungkinan dapat dialihkan kepada alamat IP yang berbahaya lewat DNS yang salah. Lalu Bad-Traffic BIND merupakan DoS attempt pada server.

Setiap harinya SQL Attack, Malware TDS, serangan pada server Wordpress dan DoS selalu terjadi di Indonesia. Dengan menggunakan algoritma APriori dan FP-Max, algoritma tersebut memberikan hasil yang sama dengan nilai minimum support sebanyak 95%. Bahkan terdapat 17 jenis dengan varian tersebut. Hal tersebut dapat terjadi, sebab dari 10 IP penyerang terbanyak, 8 IP penyerang tersebut diindikasikan sebagai botnet yang hanya memproduksi jenis-jenis malware tertentu.

Secara performa penggunaan Apache Hadoop dan Apache Hive lebih baik daripada Microsoft SQL Server dengan kondisi tanpa diindeks. Dalam pengerjaan, kueri untuk menampilkan seluruh data pada Microsoft SQL Server dapat memakan waktu sekitar 3 menit, dibandingkan Apache Hadoop yang dapat menampilkannya selama 1 menit. Pada kondisi dengan kueri lebih kompleks, Apache Hadoop dengan konfigurasi seperti yang dituliskan pada Bab 4 dapat memangkas waktu sekitar 50% daripada Microsoft SQL Server tanpa *full text indexing*. Sehingga dapat disimpulkan bahwa dengan kondisi dan

konfigurasi seperti ini, Apache Hadoop sesuai untuk tujuan *analytics.*

7.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka peneliti memberikan memiliki beberapa saran untuk para pengguna internet dan juga saran untuk penelitian. Untuk pengguna, kami memberikan saran sebagai berikut:

- Dari segi SQL Attack, Microsoft SQL Server merupakan salah satu client yang sering menjadi sasaran oleh para penyerang. Maka dari itu, bagi pengguna Microsoft SQL Server untuk memperkuat system keamanannya
- Database SQL merupakan asset yang kritis berdasarkan jumlah serangan yang terjadi dan juga frekuensi serangan yang terjadi. Oleh karena itu, para administrator database wajib memberi perhatian khusus kepada database dan aplikasinya karena SQL Attack selalu terjadi setiap hari
- Selain itu, Wordpress memiliki celah pada thimtumb.php yang perlu ditambal agar tidak dieksploitasi oleh para penyerang
- Perlunya untuk penguatan server dari sisi infrastruktur, karena serangan DoS dapat melumpuhkan server. Para administrator harus waspada apabila ada IP-IP tertentu yang mengirimkan paket besar dan stimultan sehingga mengakibatkan server menjadi crash karena tidak kuat melayani request.
- Pengguna wajib mengecek DNS yang ada pada device mereka, jangan sampai DNS tersebut merupakan DNS dari Virut DNS. Selain itu, para ISP juga harus waspada terhadap DNS palsu dan wajib menyediakan DNS yang aman bagi para penggunanya

- Pengguna wajib memasang anti malware pada setiap devicenya untuk mengurangi resiko terjadinya malware
- Adanya investigasi pada IP-IP yang memiliki serangan terbesar karena disinyalir hal tersebut merupakan IP yang digunakakn untuk kejahatan.

Untuk saran penelitian selanjutnya, penulis memberikan saran sebagai berikut :

- Nilai support pada algoritma Frequent Itemset Mining dapat diubah-ubah berdasarkan subyektivitas penulis maupun hasil eksperimen selanjutnya. Dengan menggunakan nilai support yang lebih kecil, maka akan menghasilkan pattern yang sangat banyak sehingga dapat memunculkan kemungkinan jenis-jenis malware yang lebih banyak
- Dari data yang ada, tahun sebelum dan tahun sesudahnya penelitian dapat dikembangkan dengan menggunakan algoritma *forecasting* dimana dapat meramal tren yang ada pada tahun 2013, dibandingkan dengan tahun sebelumnya dan sesudahnya
- Perlunya untuk menghitung *false positive* dan *false negative* pada setiap rule yang ada untuk memvalidasi keakuratan hasil pembacaan IDS
- Apabila menggunakan RDBMS, maka perlu untuk menggunakan Full Text Indexing untuk mempercepat performa
- Perlu untuk didiskusikan, bagaimana performa Hadoop melawan RDBMS seperti SQL Server, apakah performa Hadoop dengan banyak node computer dapat mengalahkan satu server RDBMS yang memiliki spesifikasi yang cukup tinggi. Selain itu, uji performa antara RDBMS dengan system terdistribusi perlu dilakukan dalam berbagai kondisi, baik dengan melakukan analisis log seperti penelitian ini (OLAP) maupun sebagai database transaksional (OLTP)

DAFTAR PUSTAKA

[1] d. Mehedy Masud, Data Mining Tools for Malware Detection, Washington DC: CRC Press, 2012.

[2] Symantec, "Internet Security Report Threat 2014," Symantec, 2014.

[3] Sophos, "Sophos Security Threat Report," 2013.

[4] Asia Pacific Computer Emergency Response Team, "APCERT Annual Report," 2013.

[5] Trend Micro, "TREND MICRO | TrendLabs 3Q 2013 Security Roundup," 2013..

[6] O. B. Remi-Omosowon, "Statistical Analysis For SNORT Alerts," Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK, 2010.

[7] K. P. Risto Vaarandi, "Network IDS Alert Classification with Frequent Itemset Mining and Data Clustering," in *2010 IEEE Conference on Network and Service Management*, 2010.

[8] R. R. Ravula, Classification of Malware : Using Reverse Engineering and Machine Learning Techniques, Saarbrucken: LAP Lambert Academic Publishing, 2011.

[9] P. G. A. G. T. S. A. W. C. T. V. S. Fournier-Viger, "SPMF: a Java Open-Source Pattern Mining Library," *Journal of Machine Learning Research (JMLR),* no. 15, pp. 3389-3393, 2014.

[10] R. R. a. R. Srikant, "Fast algorithms for mining association rules in large databases," IBM Almaden Research Center, San Jose, California, 1994.

[11] G. G. a. J. Zhu, "High Performance Mining of Maximal Frequent Itemsets," in *6th International Workshop on High Performance Data Mining* , 2003.

[12] M. Jazzar, Computer Network Intrusion Detection : An Integrated Approach Using Self Organizing Maps and Fuzzy Cognitive Maps, Saarbrucken: LAP Lambert Academic Publishing, 2013.

[13] D. G. L. G. M. P. S. a. V. Pearce, *CCS,* 2014.

[14] G. Tyrjubgtib, Hadoop Beginner's Guide, Birmingham: Packt Publishing, 2013.

[15] d. Ashish Thusoo, "Hive - A Petabyte Scale Data Warehouse Using Hadoop," in *IEEE 26th International Conference on Data Engineering*, California, 2010.

[16] Id-SIRTII/CC, "Ruang Lingkup ID-SIRTII/CC," [Online]. Available: http://www.idsirtii.or.id/halaman/tentang/ruang-lingkup.html. [Accessed 12 September 2015].

[17] "GeoIP2 Databases and Services," Maxmind, [Online]. Available: https://www.maxmind.com/en/geoip2-services-and-databases. [Accessed 6 Juni 2016].

[18] R. G. Alan Neville, "ZeroAccess Indepth," Symantec, 2013.

[19] J. K. S., "Frequent Item set Mining Methods," [Online]. Available: http://www-ai.cs.uni-dortmund.de/LEHRE/SEMINARE/SS09/AKTARBEITENDESDM/FOLIEN/Frequent_Itemset_Mining_Methods.pdf. [Accessed 30 September 2015].

[20] A. Moore, "K-means and Hierarchical Clustering - Tutorial Slides," 2001. [Online]. Available: http://www.autonlab.org/tutorials/kmeans11.pdf. [Accessed 30 September 2015].

BIODATA PENULIS

Penulis lahir di Mataram pada tanggal 9 Juni 1994. Penulis merupakan mahasiswa S1 Jurusan Sistem Informasi ITS pada saat buku ini ditulis. Penulis merupakan anggota dari Laboratorium Infrastruktur dan Kemanan Teknologi Informasi.

Sepanjang kehidupan dikampus, penulis aktif dalam berbagai kegiatan kemahasiswaan maupun mengikuti serangkaian kegiatan akademik. Penulis pernah menjadi wakil dari Jurusan Sistem Informasi di Dewan Perwakilan Mahasiswa ITS tahun 2014/2015. Selain itu, penulis juga aktif sebagai *volunteer* di AISINDO (Association For Information Systems Indonesia). Penulis juga aktif di kampus sebagai Asisten Laboratorium Pemrograman Sistem Informasi dan juga berbagai asisten mata kuliah seperti Bahasa Pemrograman dan Perencanaan Sumber Daya Perusahaan.

Penulis senang bergelut dengan dunia keamanan teknologi informasi, dimana juga pernah menjadi asisten dosen pada mata kuliah Keamanan Aset Informasi dan Forensika Digital. Penulis juga pernah melakukan kerja praktik pada Id-SIRTII/CC pada bidang *mobile forensics* dan melanjutkan tugas akhir dengan melakukan penelitian bersama Id-SIRTII/CC.

Penulis dapat dihubungi melalui email rowifm@outlook.com